Katedra Informatiky
Fakulta Matematiky, Fyziky a Informatiky
Univerzita Komenského, Bratislava

Matematická Logika

(spísané poznámky, draft)

`http://code.google.com/p/skripta-fmfi`

Peter Pereší ni, Milan Plžík, Pavol Struhár, Ivan Kováč

verzia zo dňa **3. júna 2011**

Úvod

Tieto poznámky obsahujú študijné materiály k predmetu Matematická logika na Fakulte matematiky, fyziky a informatiky UK.

Základ poznámok bol spísaný podľa prednášky doc. Eduarda Tomana v roku 2009. Poznámky ale nie sú oficiálny študijný materiál, preto autori neručia žiadnym spôsobom za ich aktuálnosť či vhodnosť. Navyše, obsah prednášky sa počas rôznych rokov môže meniť a preto je silne odporúčané dopísať si prípadné rozdiely medzi poznámkami a prednáškou.

Aby sme umožnoli jednoduchšie spravovanie a udržali poznámky dlhšie aktuálne, rozhodli sme sa verejne publikovať zdrojové kódy na stránke `http://code.google.com/p/skripta-fmfi`. Ak máte akékoľvek pripomienky, návrhy, opravy, môžete nám ich prostredníctvom tejto stránky oznámiť.

Za autorov, PPershing.

Obsah

Kapitola 1

Dokončenie úvodu do matematickej logiky

1.1 Prerekvizity a označenia

V tejto časti si zhrnieme najdôležitejšie označenia, pojmy a vety z prednášky "Úvod do matematickej logiky".
Označenia:

- $\vdash A$ – formula A je dokázateľná
- $\mathcal{M} \models A$ – $\mathcal{M}$ je modelom A
- $\rightarrow, \leftrightarrow$ – implikácia, ekvivalencia vo výrokovej/predikátovej logike
- $\Rightarrow, \Leftrightarrow$ – implikácia a ekvivalencia v našom jazyku

Axiómy:

A1: $A \rightarrow (B \rightarrow A)$

A2: $(A \rightarrow (B \rightarrow C)) \rightarrow [(A \rightarrow B) \rightarrow (A \rightarrow C)]$

A3: $(\neg B \rightarrow \neg A) \rightarrow (A \rightarrow B)$

A4: $(\forall x)A \rightarrow A_x[t]$

A5: $(\forall x)(A \rightarrow B) \rightarrow (A \rightarrow (\forall x)B)$ (ak x nie je voľná v A)

Pravidlá:

- Modus ponens: $\dfrac{A, A \rightarrow B}{B}$
- Pravidlo zovšeobecnenia: $\dfrac{A, x}{(\forall x)A}$
- Jednoduchý sylogizmus: $\dfrac{A, A \rightarrow B, B \rightarrow C}{C}$, resp. $\vdash (A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$.

Veta 1.1.1 (O dedukcii)

$$T \vdash A \rightarrow B \iff T, A \vdash B$$

Pozn.: V predikátovej logike ale musí na implikáciu $\Leftarrow$ navyše platiť, že na žiadnu voľnú premennú z formly A nepoužijeme v dôkaze $T, A \vdash B$ pravidlo zovšeobecnenia. Špeciálne teda ekvivalencia platí v prípade, že A je uzavretá.

Veta 1.1.2 (Postove vety a iné užitočné tvrdenia)

- $\vdash A \to A$
- $\vdash A \to \neg\neg A$
- $\vdash \neg\neg A \to A$
- $\vdash (A \to B) \to (\neg B \to \neg A)$

Lema 1.1.1 (O neutrálnej formule) *Nech $T, A \vdash B$ a tiež $T, \neg A \vdash B$. Potom $T \vdash B$.*

Lema 1.1.2 (O distribúcii kvantifikátorov) *Ak je $\vdash A \to B$, potom $\vdash (\forall x)A \to (\forall x)B$ a $\vdash (\exists x)A \to (\exists x)B$.*

Veta 1.1.3 (O ekvivalencii) *Nech formula A' vznikne z formuly A nahradením všetkých výskytov podformúl $B_1, \ldots, B_n$ v uvedenom poradí formulami $B'_1, \ldots, B'_n$. Ak platí $\vdash B_i \leftrightarrow B'_i$ pre $i \in \{1, \ldots, n\}$, potom $\vdash A \leftrightarrow A'$.*

[TODO: **vety o variantoch, zavedeni kvantifikatorov, ...**]

Lema 1.1.3 (Duálny tvar axiómy špecifikácie) $\vdash A_x[t] \to (\exists x)A$

Lema 1.1.4 (Pravidlo zavedenia existenčného kvantifikátora) *Ak $\vdash A \to B$ a x nie je voľná v B, potom $\vdash (\exists x)A \to B$.*

1.2 Prenexné tvary formúl

Ako sme mali vo výrokovej logike isté normálne tvary - konjunktívnu a disjunktívnu normálnu formu, budeme mať aj v predikátovej logike isté špeciálne tvary. Zaujímavé sú najmä prexenxná forma a ešte Skolemov normálny tvar, čo je špeciálny prípad prexenej formy. V prípade prenexného tvaru ide o preskupenie kvantifikátorov na začiatok formuly – tvar vzniká aplikovaním kvantifikátorov na otvorenú formulu.

Definícia 1.2.1 (Prenexný tvar) *Formula A je v prenexnom tvare, ak A je v nasledujúcom tvare:*

$$(Q_1 x_1)(Q_2 x_2)(Q_3 x_3) \ldots (Q_n x_n)B$$

kde $x_1, \ldots, x_n$ sú navzájom rôzne premenné, $Q_i \in \{\forall, \exists\}$ sú kvantifikátory a formula B je bez kvantifikátorov. Formulu B nazveme otvoreným jadrom formuly A, výraz $(Q_1 x_1)(Q_2 x_2)(Q_3 x_3) \ldots (Q_n x_n)$ nazveme prefixom formuly A.[1]

Poznámka 1.2.1 *(:*

- $x_1, \ldots, x_n$ sú navzájom rôzne pre vylúčenie viacnásobných kvantifikácií.
- Ak $n = 0$, tak A je otvorená a nemá prefix.
- B je najväčšia otvorená podformula formuly A.

:)

Príklad 1.2.1 Nasledujúca formula elementárnej aritmetiky je v prenexnom tvare:

$$(\forall x)(\forall y)(\exists z)(x + y = z)$$

Prefixom je $(\forall x)(\forall y)(\exists z)$ a otvorené jadro je $x + y = z$.

[1] Za prefixom nutne nasleduje iba otvorená formula. Čiže napríklad "$(\exists x)$" **nie je prefixom** $(\exists x)((\forall y)A)$**.**

Veta 1.2.1 *Nech A je ľubovoľná formula predikátovej logiky. Potom existuje formula A' v prenexnom tvare taká, že $\vdash A \leftrightarrow A'$.*

Pri prevádzaní formuly na prenexný tvar budeme využívať nasledujúce *prenexné operácie*, každá z nich nahrádza podformulu jej ekvivalentom.

a) Podformulu B nahraď jej variantom (premenovanie viazaných premenných).

b) $\neg(Qx)B$ nahraď $(\overline{Q}x)\neg B$ (negácia kvantifikátorov).

c) ak x nie je voľná v B, tak podformulu $B \to (Qx)C$ nahraď podformulou $(Qx)(B \to C)$.

d) ak x nie je voľná v C, tak $((Qx)B) \to C$ nahraď $(\overline{Q}x)(B \to C)$.

e) ak x nie je voľná v B resp. C, $\square \in \{\wedge, \vee\}$. Potom $B \square ((Qx)C)$ resp. $((Qx)B) \square C$ nahraď $(Qx)(B \square C)$.

Poznámka 1.2.2 *(: Asi stojí za zmienku upozorniť, že v časti d) x nie je voľná vo formule C narozdiel od časti c), kde x nie je voľná v B. Taktiež, medzi týmito dvoma prípadmi je zásadný rozdiel v tom, že v časti d) negujeme kvantifikátor. :)*

Lema 1.2.1 *Prenexnými operáciami dostaneme ekvivalentné formuly*

Dôkaz:

a) Veta o variantoch

b) Platí

1 $\vdash \neg(\forall x)B \leftrightarrow \underline{\neg(\forall x)\neg\neg B}$ – pretože platí $B \leftrightarrow \neg\neg B$

2 $\vdash \underline{\neg(\forall x)\neg\neg B} \leftrightarrow (\exists x)\neg B$ – pretože $(\exists x)A$ je z definície $\neg(\forall x)\neg A$.

Následným použitím vety o ekvivalencii môžeme prvú ekvivalenciu dosadiť do druhej a dostávame požadovaný výsledok. Podobne

1 $\vdash \neg(\exists x)B \leftrightarrow \underline{\neg(\exists x)\neg\neg B}$

2 $\vdash \underline{\neg(\exists x)\neg\neg B} \leftrightarrow (\forall x)\neg B$

c) Nech $Q = \forall$. Chceme ukázať $\vdash (\forall x)(B \to C) \leftrightarrow (B \to (\forall x)C)$ kde x nie je voľná v B.

$\Rightarrow$ Piata axióma predikátovej logiky.

$\Leftarrow$ 1 $\vdash (\forall x)C \to C$ – axióma špecifikácie

2 $\vdash \underbrace{(B \to (\forall x)C)}_{X} \to [\underbrace{((\forall x)C \to C)}_{Y} \to \underbrace{(B \to C)}_{Z}]$ – Jednoduchý sylogizmus

* $\vdash X \to (Y \to Z)$.

* $\vdash (X \to (Y \to Z)) \to (Y \to (X \to Z))$ – pravidlo zámeny predpokladov

3 $\vdash [(B \to (\forall x)C) \to (((\forall x)C \to C) \to (B \to C))] \to [((\forall x)C \to C) \to ((B \to (\forall x)C) \to (B \to C))]$.

4 $\vdash ((\forall x)C \to C) \to \underline{[(B \to (\forall x)C) \to (B \to C)]}$ - MP 2,3

5 $\vdash \underline{(B \to (\forall x)C) \to (B \to C)}$ - MP 1,4

6 $\vdash (B \to (\forall x)C) \to (\forall x)(B \to C)$ – pravidlo zavedenia veľkého kvantifikátora

Druhou možnosťou je $Q = \exists$. Našim cieľom je ukázať $\vdash (\exists x)(B \to C) \leftrightarrow (B \to (\exists x)C)$ za predpokladu že x nie je voľná v B.

$\Rightarrow$ 1 $\vdash C \to (\exists x)C$ – duálna verzia axiómy špecifikácie

2 $\vdash (B \to C) \to ((C \to (\exists c)C) \to (B \to (\exists x)C))$ – jednoduchý sylogizmus (JS)

3 $\vdash [(B \to C) \to ((C \to (\exists x)C) \to (B \to (\exists x)C))] \to [(C \to (\exists x)C) \to ((B \to C) \to (B \to (\exists x)C))]$ – pravidlo zámeny predpokladov

4 $\vdash ((C \to (\exists x)C) \to \underline{[(B \to C) \to (B \to (\exists x)C)]}$ – MP 2,3

5 $\vdash \underline{(B \to C) \to (B \to (\exists x)C)}$ – MP 1,4

6 $\vdash (\exists x)(B \to C) \to (B \to (\exists x)C)$ – pravidlo zavedenie existenčného kvantifikátora

$\Leftarrow$ 1 $\vdash C \to (B \to C)$ – A1

2 $\vdash (\exists x)C \to (\exists x)(B \to C)$ – pravidlo distribúcie kvantifikátorov

3 $\vdash \neg B \to (B \to C)$ – postova teoréma

4 $\vdash (B \to C) \to (\exists x)(B \to C)$ – duálny tvar axiómy špecifikácie

5 $\vdash \neg B \to (\exists x)(B \to C)$ – JS 3,4

* $\vdash [\underbrace{\neg B}_{\neg X} \to \underbrace{(\exists x)(B \to C)}_{Z}] \to [\underbrace{((\exists x)C}_{Y} \to \underbrace{(\exists x)(B \to C)}_{Z}) \to (\underbrace{(B}_{X} \to \underbrace{(\exists x)C}_{Y}) \to \underbrace{(\exists x)(B \to C)}_{Z})]$ – dokážeme neskôr

6 $\vdash [(\exists x)C \to (\exists x)(B \to C)] \to \underline{[(B \to (\exists x)C) \to (\exists x)(B \to C))]}$ – MP 5,*

7 $\vdash \underline{(B \to (\exists x)C) \to (\exists x)(B \to C))}$ – MP 2,6

Ešte treba dokázať formulu (*)

a $\neg X \to Z, Y \to Z, X \to Y, X \vdash Z$

b $\neg X \to Z, Y \to Z, X \to Y, \neg X \vdash Z$

c $\neg X \to Z, Y \to Z, X \to Y \vdash Z$ – veta o neutrálnej formule $(X, \neg X)$.

d $\vdash (\neg X \to Z) \to ((Y \to Z) \to ((X \to Y) \to Z))$ – veta o dedukcii

d) – $Q = \forall$: Ukazujeme $\vdash (\exists x)(B \to C) \leftrightarrow ((\forall x)B \to C)$ ak x nie je voľná v C.

1 $\vdash ((\forall x)B \to C) \leftrightarrow (\neg C \to \neg(\forall x)B)$

2 $\vdash ((\forall x)B \to C) \leftrightarrow (\neg C \to \neg(\forall x)\neg\neg B)$

3 $\vdash ((\forall x)B \to C) \leftrightarrow (\neg C \to (\exists x)\neg B)$

4 $\vdash \underline{(\exists x)(\neg C \to \neg B)} \leftrightarrow (\neg C \to (\exists x)\neg B)$ – časť c) tohoto dôkazu

5 $\vdash ((\forall x)B \to C) \leftrightarrow \underline{(\exists x)(\neg C \to \neg B)}$ – vetou o ekvivalentných zámenách sme dosadili 4 do 3

6 $\vdash (B \to C) \leftrightarrow (\neg C \to \neg B)$ – vieme z výrokovej logiky

7 $\vdash ((\forall x)B \to C) \leftrightarrow (\exists x)(B \to C)$ – použili sme vetu o ekvivalentných zámenách na 5,6.

– $Q = \exists$: Chceme ukázať $\vdash (\exists x)(B \to C) \leftrightarrow ((\forall x)B \to C)$ ak x nie je voľná v B. Postupujeme analogicky ako v predchádzajúcom prípade

1 $\vdash ((\exists x)B \to C) \leftrightarrow (\neg C \to \neg(\exists x)B)$

2 $\vdash ((\exists x)B \to C) \leftrightarrow (\neg C \to \neg(\exists x)\neg\neg B)$

3 $\vdash ((\exists x)B \to C) \leftrightarrow (\neg C \to (\forall x)\neg B)$

4 $\vdash \underline{(\forall x)(\neg C \to \neg B)} \leftrightarrow (\neg C \to (\forall x)\neg B)$ – časť c) tohoto dôkazu

5 $\vdash ((\exists x)B \to C) \leftrightarrow \underline{(\forall x)(\neg C \to \neg B)}$ – vetou ekvivalentných zámenách sme dosadili 4 do 3

6 $\vdash (B \to C) \leftrightarrow (\neg C \to \neg B)$ – vieme z výrokovej logiky

7 $\vdash ((\exists x)B \to C) \leftrightarrow (\forall x)(B \to C)$ – použili sme vetu o ekvivalentných zámenách na 5,6.

e) Ukazujeme $\vdash (Qx)(B \square C) \leftrightarrow (B \square (Qx)C)$, kde x nie je voľná v B. Na základe operácii c), d) toto vieme dokázať, pretože platí

$$\vdash (A \vee B) \leftrightarrow (\neg A \to B)$$
$$\vdash (A \wedge B) \leftrightarrow \neg(A \to \neg B)$$

■

Dôkaz: [Dôkaz vety 1.2.1 o prexexných tvaroch] Budeme postupovať matematickou indukciou vzhľadom na zložitosť formuly A.

- A je atomická formula. Potom je A v prenexnom tvare.
- $A = \neg B$. Na B sa vzťahuje IP, teda vieme zostrojiť B' takú, že platí $\vdash B \leftrightarrow B'$. Položíme $A' = \neg B'$ a niekoľkonásobným aplikovaním prenexnej operácie b) dostaneme A'' v správnom tvare.
- $A = B \to C$. Na B, C platí IP a teda existujú formuly B', C' v prenexnom tvare, pre ktoré platí $\vdash B \leftrightarrow B'$, $\vdash C \leftrightarrow C'$. Nech $A' = B' \to C'$. Na základe vety o ekvivalencii platí $\vdash A \leftrightarrow A'$. Teraz potrebujeme dostať A' do prenexného tvaru. Vezmime variant C'' formuly C' taký, že B', C'' nemajú žiadnu spoločnú premennú.

  $$\vdash A \leftrightarrow (B' \to C'')$$

  Teraz použijeme prenexné operácie c), d) a formulu $B' \to C''$ prevedieme do prenexného tvaru.
- $A = (\forall x)B$. Z indukčného predpokladu vyplýva existencia B', $\vdash B \leftrightarrow B'$. Môžu nastať 2 prípady
  - x nie je viazaná v B'. Položme $A' = (\forall x)B'$
  - x je viazaná v B'. Potom máme $A' = B'$.

■

Poznámka 1.2.3 *(:* Ak A obsahuje spojky $\wedge, \vee$, môžeme použiť prenexnú operáciu e) alebo formulu nahradiť ekvivaletnou formulou obsahujúcou $\neg, \to$. Ak sa vo vormule vyskytuje $\leftrightarrow$, nemôžeme priamo použiť operácie e), d) ale $A \leftrightarrow B$ prepíšeme na $(A \to B) \wedge (B \to A)$. *:)*

Príklad 1.2.2 Formula $A : B \leftrightarrow (\forall x)C$ kde x nie je voľná v B a y sa nevyskytuje v B, C.

$$\begin{aligned}
&(B \to (\forall x)C) \wedge ((\forall x)C \to B)\\
&(B \to (\forall x)C) \wedge ((\forall y)C_x[y] \to B) \text{ – podľa a)}\\
&(\forall x)(B \to C) \wedge (\exists y)(C_x[y] \to B) \text{ – podľa c), d)}\\
&(\forall x)(\exists y)((B \to C) \wedge (C_x[y] \to B)
\end{aligned}$$

Príklad 1.2.3 Formula elementárnej aritmetiky:

$$\begin{aligned}
&(\exists x)(x = y) \to (\exists x)((x = 0) \vee \neg(\exists y)(y < 0))\\
&(\exists x)(x = y) \to (\exists u)((u = 0) \vee \neg(\exists v)(v < 0)) \text{ – podľa a)}\\
&(\exists x)(x = y) \to (\exists u)((u = 0) \vee (\forall v)\neg(v < 0)) \text{ – podľa b)}\\
&(\exists x)(x = y) \to (\exists u)(\forall v)((u = 0) \vee \neg(v < 0)) \text{ – podľa e)}\\
&(\forall x)(\exists u)(\forall v)(x = y) \to ((u = 0) \vee \neg(v < 0)) \text{ – podľa c), d)}
\end{aligned}$$

1.3 Skolemov tvar formuly

Definícia 1.3.1 (Skolemov normálny tvar)[2] *Uvažujme uzevretú formulu A. Ak A má prefix $(\exists x_1)(\exists x_2)\dots(\exists x_k)(\forall x_{k+1})(\forall x_{k+2})\dots(\forall x_n)$, potom hovoríme, že formula A je vyjadrená v Skolemovom normálnom tvare, pričom $0 \leq k \leq n$.*

[2]Pozn.: Táto definícia sa mierne líši od štandardnej, v tej sa nemôžu vyskytovať žiadne existenčné kvantifikátory

Veta 1.3.1 *Nech A je formula predikátovej logiky. Potom k nej môžeme zostrojiť formulu A' v Skolemovom normálnom tvare, pričom platí $\vdash A \iff \vdash A'$.*

Poznámka 1.3.1 *(:* Všimnime si, že predchádzajúca veta nehovorí nič o existencii formuly A' takej, že $\vdash A \leftrightarrow A'$ ako to bolo u prenexného tvaru. Taká formula totiž v prípade Skolemovho normálneho tvaru nemusí existovať. *:)*

Definícia 1.3.2 (Hodnosť formuly) *Uvažujme formulu A vyjadrenú v prenexnom tvare. Potom pod hodnosťou formuly A označíme počet veľkých kvantifikátorov, ktoré v prefixe predchádzajú posledný existenčný kvantifikátor (počítame zľava doprava).*

Príklad 1.3.1 Uvažujme formulu

$$(\forall x)(\forall y)(\exists z)(\forall u)(\exists w)(\exists v)(\forall s)(\forall t)A$$

Jej hodnosť je 3.

Dôkaz: [Vety 1.3.1 o Skolemovom tvare] Budeme predpokladať, že A je uzavretá (Podľa vety o uzávere platí, že je dokázateľné $\vdash A$ práve vtedy, keď je dokázateľný uzáver formuly A) a taktiež že je v prenexnom tvare (to vieme zabezpečiť). Dôkaz bude prebiehať matematickou indukciou vzhľadom na hodnosť m formuly A.

- $m = 0$ - A je v Skolemovom normálnom tvare
- IP: tvrdenie vety platí pre každú formulu ktorej hodnosť je $m-1$. Nech je teda A tvaru

$$A : (\exists x_1)(\exists x_2)\dots(\exists x_n)(\forall y)B(x_1, x_2, \dots, x_n, y) \tag{1.1}$$

kde B nie je nutne bezkvantifikátorová (a je v prenexnom tvare). Pretože A je uzavretá, v B sú voľné iba $x_1, x_2, \dots, x_n, y$. Keďže hodnosť A je m, tak vo formule B poslednému existenčnému kvantifikátoru predchádza práve $m-1$ všeobecných kvantifikátorov. Nech P^{n+1} je $(n+1)$-árny predikát, ktorý sa nevyskytuje v A (a teda ani B). Uvažujme nasledujúcu formulu

$$A^* : (\exists x_1)(\exists x_2)\dots(\exists x_n)\Big[(\forall y)[B(x_1, \dots, x_n, y) \to P^{(n+1)}(x_1, \dots, x_n, y)] \to (\forall y)P^{(n+1)}(x_1, \dots, x_n, y)\Big] \tag{1.2}$$

Postupne ukážeme, že $\vdash A \iff \vdash A^*$.

$\Rightarrow$

0 $\vdash A$

1 $\vdash (B \to P^{(n+1)}) \to (B \to P^{(n+1)})$ – inštancia $X \to X$.

2 $\vdash (X \to (Y \to Z)) \to (Y \to (X \to Z))$ – veta o zámene predpokladov

3 $\vdash [\underbrace{(B \to P^{(n+1)})}_{X} \to (\underbrace{B}_{Y} \to \underbrace{P^{(n+1)}}_{Z})] \to [\underbrace{B}_{Y} \to (\underbrace{(B \to P^{(n+1)})}_{X} \to \underbrace{P^{(n+1)}}_{Z})]$ – inštancia kroku 2

4 $\vdash B \to ((B \to P^{(n+1)}) \to P^{(n+1)})$ – MP 1,3.[3]

x $\vdash (\forall y)B \to (\forall y)((B \to P^{(n+1)}) \to P^{(n+1)})$ – veta o distribúcii kvantifikátorov aplikovaná na 4

y $(\forall y)((B \to P^{(n+1)}) \to P^{(n+1)}) \to ((\forall y)(B \to P^{(n+1)}) \to (\forall y)P^{(n+1)})$ – Ukážeme nasledovne:

a $(\forall x)(X \to Y) \vdash (\forall x)(X \to Y)$ – predpoklad je vždy dokázateľný

b $\vdash (\forall x)(X \to Y) \to (X \to Y)$ – axióma špecifikácie

c $(\forall x)(X \to Y) \vdash X \to Y$ – MP a,b

[3] Toman: Ideme to obliecť, zatiaľ je obnažená.

d $(\forall x)(X \to Y) \vdash (\forall x)X \to (\forall x)Y$ – pravidlo zavedenia všeobecného kvantifikátora aplikované na c

e $\vdash (\forall x)(X \to Y) \to ((\forall x)X \to (\forall x)Y)$ – veta o dedukcii v predikátovej logike.[4]

5 $\vdash (\forall y)B \to ((\forall y)(B \to P^{(n+1)}) \to (\forall y)P^{(n+1)})$ – pravidlo jednoduchého sylogizmu aplikované na x,y

z $\vdash (\forall x_1)(\forall x_2)\dots(\forall x_n)\left[(\forall y)B \to ((\forall y)(B \to P^{(n+1)}) \to (\forall y)P^{(n+1)})\right]$ – n-krát aplikované pravidlo zovšeobecnenia na krok 5

6 $\vdash (\exists x_1)(\exists x_2)\dots(\exists x_n)(\forall y)B \to (\exists x_1)(\exists x_2)\dots(\exists x_n)\left[(\forall y)(B \to P^{(n+1)}) \to (\forall y)P^{(n+1)})\right]$ – n-krát použijeme $\vdash (\forall x)(A \to B) \to ((\exists x)A \to (\exists x)B)$, čo sa dá dokázať nasledovne:

c $(\forall x)(X \to Y) \vdash X \to Y$ – už sme mali

j $\vdash Y \to (\exists x)Y$ – duálny tvar axiómy špecifikácie

k $(\forall x)(X \to Y) \vdash X \to (\exists x)Y$ – JS c,j

l $(\forall x)(X \to Y) \vdash (\exists x)X \to (\exists x)Y$ – pravidlo zavedenia existenčného kvantifikátora, x nie je voľné v $(\exists x)Y$.

m $\vdash (\forall x)(X \to Y) \to (\exists x)X \to (\exists x)Y$ – Veta o dedukcii, čitateľ si môže premyslieť, že ju môžeme použiť

7 $\vdash (\exists x_1)(\exists x_2)\dots(\exists x_n)\left[(\forall y)(B \to P^{(n+1)}) \to (\forall y)P^{(n+1)}\right]$ – MP indukčného predpokladu a 6

$\Leftarrow$ Predpokladáme, že je dokázateľné $\vdash A^* : (\exists x_1)(\exists x_2)\dots(\exists x_n)[(\forall y)(B \to P^{(n+1)}) \to (\forall y)P^{(n+1)}]$. Treba si uvedomiť, že na predikát $P^{(n+1)}$ nekladieme žiadne nároky a teda je to dokázateľné pre ľubovoľný taký predikát. No ale formula B sa dá chápať ako špeciálny prípad $(n+1)$-árneho predikátu. Preto bude dokázateľná aj inštancia formuly A^*, ktorá vyzerá nasledovne: $\vdash (\exists x_1)(\exists x_2)\dots(\exists x_n)[(\forall y)(B \to B) \to (\forall y)B]$

1 $\vdash (\exists x_1)(\exists x_2)\dots(\exists x_n)[(\forall y)(B \to B) \to (\forall y)B]$

2 $\vdash (\exists x)(X \to Y) \to ((\forall x)X \to (\exists x)Y)$ – dá sa dokázať napríklad takto:

- $\vdash X \to (\neg Y \to \neg(X \to Y))$
- $\vdash (\forall x)X \to (\forall x)(\neg Y \to \neg(X \to Y))$ – veta o zavedení všeobecných kvantifikátorov
- $(\forall x)X \vdash (\forall x)(\neg Y \to \neg(X \to Y))$ – veta o dedukcii
- $(\forall x)X \vdash (\forall x)\neg Y \to (\forall x)\neg(X \to Y)$ – veta o distribúcii kvantifikátorov[5]
- $(\forall x)X \vdash \neg(\forall x)\neg(X \to Y) \to \neg(\forall x)\neg Y$ – obmena implikácie
- $(\forall x)X \vdash (\exists x)(X \to Y) \to (\exists x)Y$ – nahradenie kvantifikátorov
- $\vdash (\exists x)(X \to Y) \to (\forall x)X \to (\exists x)Y$ – 2 krát veta o dedukcii

3 $\vdash (\exists x_1)(\exists x_2)\dots(\exists x_n)[(\forall y)(B \to B) \to (\forall y)B] \to [(\forall x_1)(\forall x_2)\dots(\forall x_n)(\forall y)(B \to B) \to (\exists x_1)(\exists x_2)\dots(\exists x_n)(\forall y)B]$ – n-krát využijeme 2 nasledujúcim štýlom: Použijeme na dané pravidlo vetu o zavedení existenčného kvantifikátora. Následne, pravú stranu hlavnej implikácie vidíme ako kandidáta na krok 2. Preto ju na novom riadku rozpíšeme podľa tohoto pravidla a následne použitím jednoduchého sylogizmu tieto 2 riadky zložíme. Tím dostaneme variantu 2 s pridanou ďalšou premennou a toto opakujeme príslušný počet krát.

4 $\vdash (\forall x_1)(\forall x_2)\dots(\forall x_n)(\forall y)(B \to B) \to (\exists x_1)(\exists x_2)\dots(\exists x_n)(\forall y)B$. – MP 1,3

5 $\vdash (\forall x_1)(\forall x_2)\dots(\forall x_n)(\forall y)(B \to B)$ – $(n+1)$-krát pravidlo zovšeobecnenia použité na dokázateľnú formulu $\vdash B \to B$.

[4] Pozor, treba si riadne premyslieť, že ju môžeme použiť. Totiž, v dôkaze d sme nikne nepoužili pravidlo zovšeobecnenia na premennú, ktorá by bola voľná v $(\forall x)(X \to Y)$ – použili sme to iba na premennú x a tá je viazaná.

[5] formálne by sme mali ešte spraviť medzikrok $(\forall x)X \vdash \neg Y \to \neg(X \to Y)$

$6 \vdash \underline{(\exists x_1)(\exists x_2)\dots(\exists x_n)(\forall y)B}$ – MP 4,5

Ešte potrebujeme transformovať formulu A^* na formulu s hodnosťou $m-1$. Vieme, že B je v prenexnom tvare (predpokladami sme to hneď na začiatku) a teda ju môžeme zapísať ako $B : (Q_1 z_1)(Q_2 z_2)\dots(Q_l z_l)C$, kde C je formula bez kvantifikátorov. Vieme, že hodnosť B, resp. hodnosť jej prefixu $(Q_1 z_1)(Q_2 z_2)\dots(Q_l z_l)$ je $m-1$ nakoľko hodnosť A je m a v A sa pred B nachádza jeden všeobecný kvantifikátor.

$A^* = (\exists x_1)(\exists x_2)\dots(\exists x_n)\,[(\forall y)\,[(Q_1 z_1)(Q_2 z_2)\dots(Q_l z_l)C \to P^{(n+1)}] \to (\forall y)P^{(n+1)}]$

$\Leftrightarrow (\exists x_1)(\exists x_2)\dots(\exists x_n)\,[(\forall y)(\overline{Q_1} z_1)(\overline{Q_2} z_2)\dots(\overline{Q_l} z_l)\,[C \to P^{(n+1)}] \to (\forall u)P^{(n+1)}]$ – veta o variantoch (druhé y premenované na u) + l prenexných operácií d)

$\Leftrightarrow (\exists x_1)(\exists x_2)\dots(\exists x_n)(\exists y)\,[(\overline{Q_1} z_1)(\overline{Q_2} z_2)\dots(\overline{Q_l} z_l)\,[C \to P^{(n+1)}] \to (\forall u)P^{(n+1)}]$ – prenexná operácia d) aplikovaná na y

$\Leftrightarrow (\exists x_1)(\exists x_2)\dots(\exists x_n)(\exists y)(Q_1 z_1)(Q_2 z_2)\dots(Q_l z_l)\,[\,[C \to P^{(n+1)}] \to (\forall u)P^{(n+1)}]$ – l-krát prenexná operácia d)

$\Leftrightarrow (\exists x_1)(\exists x_2)\dots(\exists x_n)(\exists y)(Q_1 z_1)(Q_2 z_2)\dots(Q_l z_l)(\forall u)\,[\,[C \to P^{(n+1)}] \to P^{(n+1)}]$ – prenexná operácia c) aplikovaná na u

Posledná formula má hodnosť $m-1$ a je v prenexnom tvare. Tým pádom ju vieme podľa indukčného predpokladu previesť na Skolemov normálny tvar.

■

1.4 Predikátová logika s rovnosťou

Predikátovú logiku môžeme rozšíriť o nové axiómy, ktoré budú hovoriť o predikáte "=".

Axiómy rovnosti:

R1: ak x je premenná, potom formula $x = x$ je axióma

R2: ak $x_1, \dots, x_k, y_1, \dots, y_k$ sú premenné a f je k-árny funkčný symbol, potom je axiómou formula

$$(x_1 = y_1) \to ((x_2 = y_2) \to (\dots \to ((x_k = y_k) \to [f(x_1, \dots, x_k) = f(y_1, \dots, y_k)] \dots)))$$

R3: ak $x_1, \dots, x_k, y_1, \dots y_k$ sú premenné a P je k-árny predikátový symbol, potom je axiómou formula

$$(x_1 = y_1) \to ((x_2 = y_2) \to (\dots \to ((x_k = y_k) \to [P(x_1, \dots, x_k) \to P(y_1, \dots, y_k)] \dots)))$$

Príklad 1.4.1 (Teória neostrého čiastočného usporiadania $\leq$)

1. $(\forall x)\langle x, x\rangle \in \varphi$ – identita
2. $(\forall x)(\forall y)[(\langle x, y\rangle \in \varphi \wedge \langle y, x\rangle \in \varphi) \to (x = y)]$ – antisymetrickosť
3. $(\forall x)(\forall y)(\forall z)[(\langle x, y\rangle \in \varphi \wedge \langle y, z\rangle \in \varphi) \to \langle x, z\rangle \in \varphi]$ – tranzitívnosť[6]

Ak pridáme trichotomickosť, dostaneme teóriu neostrého usporiadania:

4. $(\forall x)(\forall y)[x \neq y \to (\langle x, y\rangle \in \varphi \vee \langle y, x\rangle \in \varphi)]$

4' $(\forall x)(\forall y)[x = y \vee \langle x, y\rangle \in \varphi \vee \langle y, x\rangle \in \varphi]$

[6]Pozn.: Axiómu môžeme uvádzať aj v ekvivalentnom tvare $(\forall x)(\forall y)(\forall z)[\langle x, y\rangle \in \varphi \to (\langle y, z\rangle \in \varphi \to \langle x, z\rangle \in \varphi)]$. Inak povedané, $(A \wedge B) \to C$ sme nahradili $A \to (B \to C)$.

Lema 1.4.1 *Rovnosť je symetrická a tranzitívna.*

1 $\vdash (x = y) \to (y = x)$ – *symetria*

2 $\vdash (x = y) \to ((y = z) \to (x = z))$ – *tranzitívnosť*

Dôkaz:

- Symetria:

  1 $\vdash (x = y) \to ((x = x) \to ((x = x) \to (y = x)))$ pretože
  $\vdash (x_1 = y_1) \to ((x_2 = y_2) \to ((x_1 = x_2) \to (y_1 = y_2)))$ je inštancia R3

  2 $\vdash A \to (B \to (B \to C))$.

  3 $\vdash B \to (B \to (A \to C))$ – 2x použité pravidlo zámeny predpokladov + veta o dedukcii

  4 $\vdash (x = x) \to (x = x) \to (x = y) \to (y = x)$

  5 $\vdash x = x$ – R1

  6 $\vdash (x = y) \to (y = x)$ – 2x MP na 5,4

- Tranzitívnosť:

  1 $\vdash (y = x) \to ((z = z) \to ((y = z) \to (x = z)))$, pretože
  $\vdash (x_1 = y_1) \to ((x_2 = y_2) \to ((x_1 = x_2) \to (y_1 = y_2)))$ je inštancia R3.

  2 $\vdash A \to (B \to (C \to D))$

  3 $\vdash B \to (A \to (C \to D))$ – pravidlo zámeny predpokladov

  4 $\vdash (z = z) \to [(y = x) \to ((y = z) \to (x = z))]$

  5 $\vdash z = z$ – R1

  6 $\vdash (y = x) \to ((y = z) \to (x = z))$ – MP 4,5

  7 $\vdash (A \to B) \to ((B \to C)) \to (A \to C))$ – JS

  8 $\vdash [(x = y) \to (y = x)] \to \Big[[(y = x) \to ((y = z) \to (x = z))] \to [(x = y) \to ((y = z) \to (x = z)))]\Big]$
  – inštancia 7

  9 $\vdash (x = y) \to (y = x)$ – symetria

  10 $\vdash [(y = x) \to ((y = z) \to (x = z))] \to [(x = y) \to ((y = z) \to (x = z))]$ – MP 9,8

  11 $\vdash (x = y) \to ((y = z) \to (x = z))$ – MP 6,10

■

Veta 1.4.1 *Nech* $t_1, \ldots, t_n, s_1, \ldots, s_n$ *sú termy, pričom platí* $\forall i \in \{1, \ldots, n\} : \vdash t_i = s_i$. *Potom*

i) Ak t *je term, ktorý vznikne z termu* s *nahradením niektorých výskytov termov* s_i *za* t_i, *potom* $\vdash t = s$.

ii) Ak A' *je formula, ktorá vznikne z formuly* A *dosadením* t_i *za niektoré termy* s_i, *okrem prípadov, keď* t_i *je premenná* x *v kvantifikácii* $(\forall x)$ *resp.* $(\exists x)$. *Potom* $\vdash A \leftrightarrow A'$.

Dôkaz:

i) Dôkaz matematickou indukciou vzhľadom na zložitosť termu t.

- Nech t je premenná alebo t je s_i pre nejaké i. Potom zjavne $\vdash t = s_i$.
- Nech term t je $f(r_1, \ldots, r_k)$, term s je $f(r'_1, \ldots, r'_k)$. Pre $r_1, \ldots, r_k$ platí IP, čize $\vdash r_i = r'_i$. Potom $\vdash (r_1 = r'_1) \to \ldots \to (r_k = r'_k) \to (f(r_1, \ldots, r_k) = f(r'_1, \ldots, r'_k))$, čo k-násobným použitím MP na indukčný predpoklad vedie k $\vdash f(r_1, \ldots, r_k) = f(r'_1, \ldots, r'_k)$.

ii) Zámena termov prebieha len v atomických podformulách formuly A (každý term je časťou nejakej atomickej podformuly). Máme 2 možnosti, ako vyzerá atomická podformula:

- Nech P je atomická podformula tvaru $P(r_1, \ldots, r_l)$. Potom po zámene dostaneme z $P(r_1, \ldots, r_k)$ formulu $P' : P(r'_1, \ldots, r'_k)$. Chceme ukázať $\vdash P(r_1, \ldots, r_k) \leftrightarrow P(r'_1, \ldots, r'_k)$, ak vieme, že podľa IP platí $\forall i :\vdash r_i = r'_i$

  $\Rightarrow$: · $\vdash (r_1 = r'_1) \to (r_2 = r'_2) \to \ldots \to (r_k = r'_k) \to (P(r_1, \ldots, r_k) \to P(r'_1, \ldots, r'_k))$ – inštancia R3
  · $\vdash r_i = r'_i$ – IP
  · $\vdash P(r_1, \ldots, r_k) \to P(r'_1, \ldots, r'_k)$ – k-krát MP

  $\Leftarrow$: · $\vdash (r'_1 = r_1) \to (r'_2 = r_2) \to \ldots \to (r'_k = r_k) \to (P(r'_1, \ldots, r'_k) \to P(r_1, \ldots, r_k))$ – inštancia R3
  · $\vdash r'_i = r_i$ – IP + symetria
  · $\vdash P(r'_1, \ldots, r'_k) \to P(r_1, \ldots, r_k)$ – k-krát MP

- Nech atomická podformula je tvaru $r_1 = r_2$. Tento prípad sa dá ukázať podobne ako predchádzajúci, na prednáške bol ale iný dokaz: Chceme ukázať $\vdash r_1 = r_2 \leftrightarrow r'_1 = r'_2$.

  $\Rightarrow$: · $\vdash r_1 = r'_1$ – IP
  · $\vdash r_2 = r'_2$ – IP
  · $\vdash r_1 = r_2 \to (r_2 = r'_2 \to r_1 = r'_2)$ – tranzitívnosť
  · $r_1 = r_2 \vdash r_1 = r'_2$ – VD + MP
  · $r_1 = r_2 \vdash r'_2 = r_1$ – symetria + MP
  · $\vdash r'_2 = r_1 \to (r_1 = r'_1 \to r'_2 = r'_1)$ – tranzitívnosť
  · $r_1 = r_2 \vdash r'_2 = r'_1$ – 2-krát MP
  · $r_1 = r_2 \vdash r'_1 = r'_2$ – symetria + MP
  · $\vdash r_1 = r_2 \to r'_1 = r'_2$ – VD

  $\Leftarrow$: · $\vdash r_1 = r'_1$ – IP
  · $\vdash r_2 = r'_2$ – IP
  · $\vdash r'_1 = r'_2 \to (r'_2 = r_2 \to r'_1 = r_2)$ – tranzitívnosť
  · $r'_1 = r'_2 \vdash r'_1 = r_2$ – VD + MP
  · $\vdash r_1 = r'_1 \to (r'_1 = r_2 \to r_1 = r_2)$ – tranzitívnosť
  · $r'_1 = r'_2 \vdash r_1 = r_2$ – 2xMP
  · $\vdash r'_1 = r'_2 \to r_1 = r_2$ – VD

  Dokázali sme, že atomické podformuly sú ekvivalentné. Spolu s vetou o ekvivalencii to ale znamená, že aj pôvodné formuly sú ekvivalentné.

■

Veta 1.4.2 *Majme term t, termy $t_1, \ldots, t_n, s_1, \ldots, s_n$ a formulu A. Potom platí*

i) $\vdash t_1 = s_2 \to t_2 = s_2 \to t_n = s_n \to (t[t_1, \ldots, t_n] = t[s_1, \ldots, s_n])$.

ii) $\vdash t_1 = s_2 \to t_2 = s_2 \to t_n = s_n \to (A[t_1, \ldots, t_n] \leftrightarrow A[s_1, \ldots, s_n])$.

Ak navyše x je premenná, ktorá nie je obsiahnutá v terme t, potom platí

iii) $\vdash A_x[t] \leftrightarrow (\forall x)((x = t) \to A)$

iv) $\vdash A_x[t] \leftrightarrow (\exists x)((x = t) \wedge A)$

Dôkaz:

i),ii) Ak $t_1, \ldots, t_n, s_1, \ldots, s_n$ neobsahujú premenné, tak to vyplýva priamo z predchádzajúcej vety a vety o dedukcii. V prípade, že tieto termy obsahujú premenné, tieto premenné nahradíme rôznymi konštantami, použijeme vetu o konštantách,[7] predchádzajúcu vetu a vetu o dedukcii.

iii) $\Rightarrow$:
- $* \vdash x = t \to (A \leftrightarrow A_x[t])$ – podľa ii).
- $* \vdash \underbrace{x = t}_{X} \to (\underbrace{A_x[t]}_{Y} \to \underbrace{A}_{Z})$ – platí totiž $\vdash (B \to (C \leftrightarrow D)) \to (B \to (D \to C))$
- $* \ (X \to (Y \to Z)) \to (Y \to (X \to Z))$ – pravidlo zámeny predpokladov
- $* \vdash A_x[t] \to (x = t \to A)$ – MP na pravidlo zámeny predpokladov
- $* \vdash A_x[t] \to (\forall x)(x = t \to A)$ – pravidlo zavedenia všeobecného kvantifikátora

$\Leftarrow$:
- $* \vdash \underbrace{(\forall x)(x = t \to A)}_{X} \to (\underbrace{(t = t)}_{Y} \to \underbrace{A_x[t]}_{Z})$ – Axióma špecifikácie
- $* \ (X \to (Y \to Z)) \to (Y \to (X \to Z))$ – pravidlo zámeny predpokladov
- $* \vdash (t = t) \to ((\forall x)((x = t) \to A) \to A_x[t])$ – MP
- $* \vdash t = t$ – axióma R1
- $* \vdash (\forall x)((x = t) \to A) \to A_x[t]$ – MP

iv)
1. $\vdash (\forall x)((x = t) \to A) \leftrightarrow A_x[t]$ – iii)
2. $\vdash (\forall x)((x = t) \to \neg A) \leftrightarrow \neg A_x[t]$ – inštancia 1
3. $\vdash \neg\neg A_x[t] \leftrightarrow \neg(\forall x)((x = t) \to \neg A)$ – obmena ekvivalencie
4. $\vdash A_x[t] \leftrightarrow (\exists x)\neg((x = t) \to \neg A)$ – odstránenie $\neg\neg$ a zámena kvantifikátora
5. $\vdash \neg(X \to \neg Y) \leftrightarrow (X \wedge Y)$ – rozpísanie $\wedge$
6. $\vdash A_x[t] \leftrightarrow (\exists x)((x = t) \wedge A)$ – veta o ekvivalencii aplikovaná na 4,5

■

[7] Veta o konštantách hovorí, že $T \vdash A \iff T \vdash A[c_1, \ldots, c_m]$ kde $c_1, \ldots, c_m$ sú nové konštanty. Inak povedané, to, že niečo vieme dokázať s premennými je ekvivalentné tomu, že to vieme dokázať ak premenné nahradíme novými konštantami

Kapitola 2

Matematická logika

2.1 Pravdivosť a dokázateľnosť

Definícia 2.1.1 (Logická platnosť formuly) *Nech L je jazyk prvého rádu a A je formula jazyka L. Hovoríme, že formula A je logicky platná, označujeme $\models A$, ak je splnená v ľubovoľnej realizácii $\mathcal{M}$ jazyka L.*

$$\begin{aligned} \mathcal{M} &\models A[e] \quad \forall \mathcal{M} \\ \mathcal{M} &\models A \\ &\models A \end{aligned}$$

Poznámka 2.1.1 *(:* Formula A je logicky platná, práve vtedy, keď je pravdivá bez ohľadu na realizáciu symbolov jazyka L. *:)*

Definícia 2.1.2 (Teória) *Nech L je jazyk prvého rádu a T je množina formúl jazyka L. Hovoríme, že T je teória 1. rádu predikátovej logiky s jazykom L (t.j. množina formúl T je množina axióm teórie).*

Definícia 2.1.3 (Model teórie) *Nech T je teória v jazyku L, $\mathcal{M}$ je realizácia jazyka L. Hovoríme, že $\mathcal{M}$ je modelom teórie T (označujeme $\mathcal{M} \models T$), ak pre každú formulu A patriacu T platí $\mathcal{M} \models A$.*

Definícia 2.1.4 (Tautologický dôsledok) *Hovoríme, že formula A je sémantickým/tautologickým dôsledkom (vetou teórie) množiny formúl T, resp. A je T-platná, ak A je splnená v každom modeli teórie T. Túto skutočnosť označujeme $T \models A$.*

Príklad 2.1.1 (Teória ostrého usporiadania) Majme predikát $<$ na množine $\mathbb{N}$, tak, že platí

1. $(\forall x)(\forall y)((x < y) \rightarrow \neg(y < x))$ – asymetrickosť
2. $(\forall x)(\forall y)(\forall z)(((x < y) \wedge (y < z)) \rightarrow (x < z))$ – tranzitívnosť
3. $(\forall x)(\forall y)((x \neq y) \rightarrow ((x < y) \vee (y < x)))$ – trichotomickosť

Ak sú splnené axiómy 1,2, tak daná množina je modelom *čiastočného* ostrého. usporiadania. Ak je navyše splnená aj axióma 3, množina tvorí teóriu ostrého usporiadania.

Poznámka 2.1.2 *(:* Pozornému čitateľovi isto neušiel fakt, že sme už raz mali teóriu usporiadania a mali sme v nej až 4 axiómy. Poznamenajme, že vtedy išlo o teóriu neostrého usporiadania $\leq$ a chýbajúca axióma bola

$$(\forall x)(x \leq x)$$

:)

Príklad 2.1.2 (Elementárna aritmetika) Jazyk prvého rádu rozšírme o nasledujúce symboly:

- 0 – konštanta (nulárny funkčný symbol),
- S – nasledovník (unárny funkčný symbol), čiže $S(x) = x + 1$
- $+, *$ – binárne funkčné symboly

Axiómy elementárnej aritmetiky:

1. $\neg(S(x) = 0)$
2. $(S(x) = S(y)) \rightarrow (x = y)$
3. $(x + 0) = x$
4. $(x + S(y)) = (S(x) + y)$
5. $(x * 0) = 0$
6. $(x * S(y)) = ((x * y) + x)$

Zoberme si realizáciu $\mathcal{N} = \langle \mathbb{N}_0, 0, S, +, * \rangle$ kde $\mathbb{N}_0 = \{0, 1, 2, \dots\}$. Potom $\mathcal{N}$ je model pre elementárnu aritmetiku, zvykne sa označovať aj ako štandardný model. Takejto aritmetike sa hovorí Robinsonova aritmetika. Ak pridáme axiómu indukcie, dostaneme Peanovu aritmetiku.

Poznámka 2.1.3 *(:* Nevšímajme si nachvíľu axiómy, ale iba relačnú štruktúru $\mathcal{N} = \langle \mathbb{N}_0, 0, S, +, * \rangle$. Zoberme namiesto S konštantu 1. Čiže $\mathcal{N}' = \langle \mathbb{N}_0, 0, 1, +, * \rangle$. $\mathcal{N}'$ realizuje jazyk teórie telies. Lenže $\mathcal{N}'$ nie je modelom tohoto jazyka – na to, aby daná realizácia bola modelom, muselo by platiť, že každá formula T je splnená v danej realizácii. V našom prípade, v každom telese platí $\vdash \neg(S(S(0)) = S(0))$ (inak povedané, $2 \neq 1$, ak má teleso charakteristiku viac ako 2, v prípade charakteristiky 2 je to $0 \neq 1$). Nuž ale v $\mathcal{N}'$ je splnená formula $S(S(0)) = S(0)$, lebo sa realizuje ako $1 = 1$. *:)*

Príklad 2.1.3 (Teória grúp) Špeciálne symboly sú $+$ (binárna operácia), $-$ (unárna operácia – inverzný prvok) a 0 (konštanta – neutrálny prvok). Axiómy sú:

1. $((x + y) + z) = (x + (y + z))$ – asociativita
2. $(x + 0) = (0 + x) = x$ – existuje neutrálny prvok označený ako 0
3. $x + (-x) = 0 = (-x) + x$ – existujú (ľavé a pravé) inverzné prvky

Ďalším cieľom je stotožniť dokázateľné formuly s tautológiami.

Veta 2.1.1 (O korektnosti) *Ak T je teória v jazyku L a ak formula A je taká, že $T \vdash A$, potom $T \models A$.*

Dôkaz: Nech $A_1, A_2, \dots, A_n \equiv A$ je odvodenie (dôkaz) formuly A z predpokladov T (v teórii T). Nech $\mathcal{M}$ nech je ľubovoľný model teórie T (čiže platí $\mathcal{M} \models T$). Ukážeme (indukciou podľa dĺžky dôkazu), že ak platí $\forall j < i : \mathcal{M} \models A_j$, potom platí aj platí $\mathcal{M} \models A_i$

Do dôkazu sa A_i môže dostať niekoľkými spôsobmi:

1. $A_i \in T, \mathcal{M}$ je model T. Potom $\mathcal{M} \models A_i$ a teda $T \models A_i$
2. A_i sa dostane do dôkazu ako axióma predikátovej logiky:
   (a) A_i je axióma výrokovej logiky – je poskladaná z atomických formúl a logických spojok $\neg$ a $\rightarrow$. Potom A_i je tautológia výrokovej logiky a ak je formula tautológia, jej pravdivostná hodnota nezávisí od ohodnotenia premenných: $\mathcal{M} \models A_i$, čiže $\mathcal{M} \models A_i[e]$.

(b) A_i je axioma špecifikácie, teda je tvaru $A_i : (\forall x)B \to B_x[t]$, kde t je substitúcia za x do B. Chceme ukázať, že formula bude pravdivá pri každom ohodnotení e. Zaujíma nás prípad, kedy $(\forall x)B$ je pravdivý.[1] To znamená, že pre ľubovoľné indivíduum m platí (z Tarského definície) $B[e(x/m)]$, teda $e(x) = m$.
Tvrdenie zo zimného semestra: Ak platí $\forall i : t_i[e] = m_i$, potom

$$\mathcal{M} \models A_{x_1,\dots x_n}[t_1,\dots t_n][e] \iff \mathcal{M} \models A[e(x_1/m_1,\dots x_n/m_n)]$$

Teda namiesto $B_x[t][e]$, vieme použiť $B[e(x/m)]$. Táto formula je ale pravdivá v $\mathcal{M}$ (viď vyššie).

(c) $A_i : (\forall x)(B \to C) \to (B \to (\forall x)C)$ a x nie je voľná v B. Mali by sme dokázať, že platí $\mathcal{M} \models A_i$. Zaujímavý prípad je, keď $\mathcal{M} \models (B \to C)[e(x/m)]$ platí pre ľubovoľné indivíduum m, vtedy sa pozeráme na platnosť $(B \to (\forall x)C)$. Posledná formula je ale ekvivalentná s $\neg B \vee (\forall x)C$. Dôležitý je tiež predpoklad, že x nie je voľná v B, a teda B nezávisí od jej ohodnotenia. Ak B nie je pravdivá, tak disjunkcia je pravdivá a problém je vyriešený. Ak by B bola pravdivá, tak by malo byť $(\forall x)C$ pravdivé. Lenže to musí byť, inak by neplatilo $(\forall x)(B \to C)$.

3. A_i je niektorá axióma rovnosti:

(a) $A_i : x = x$. Potom $A_i[e]$ je $m = m$ a teda pri každom ohodnotení $\mathcal{M} \models A_i$.

(b) $A_i : (x_1 = y_1) \to (x_2 = y_2) \to \dots \to [f(x_1,\dots,x_n) = f(y_1,\dots,y_n)]$. Zaujíma nás prípad, keď $e(x_i) = e(y_i)$, teda $e(x_i) = e(y_i) = m_i$. Vtedy dostávame

$$m_1 = m_1 \to m_2 = m_2 \to \dots \to [f(m_1,\dots,m_n) = f(m_1,\dots,m_n)]$$

(c) $A_i : (x_1 = y_1) \to (x_2 = y_2) \to \dots \to [P(x_1,\dots,x_n) \to P(y_1,\dots,y_n)]$. Zaujíma nás opäť prípad, keď x_i aj y_i reprezentujeme rovnakým indivíduom: $e(x_i/m_i)$ a $e(y_i/m_i)$. Potom $(m_1,\dots,m_n)$ buď je alebo nie je v relácii P a implikácia $P \to P$ bude pravdivá.

4. A_i dostávame ako výsledok odvodzovacieho pravidla.

(a) Modus Ponens: Vieme $T \vdash A_j,\ T \vdash A_j \to A_i$. Podľa IP platí $T \models A_j,\ T \models A_j \to A_i$ a vďaka korektnosti MP teda aj $T \models A_i$.

(b) Pravidlo zovšebecnenia: $A_i : (\forall x)A_j$. Z IP platí $T \models A_j$ a teda $\mathcal{M} \models A_i[e(x/m)]$ pre ľubovoľné indivíduum m. Tým pádom ale $T \models (\forall x)A_j$.

■

Príklad 2.1.4 Uvažujme elementárnu aritmetiku, ktorá má svoj štandardný model $\mathcal{M}$. Uvažujme formulu $x = 0$ v N.

- Nech $e(x) = m$ kde $m \neq 0$. Potom formula $A : x = 0$ nie je splnená pre ohodnotenie e a teda $\mathcal{M} \not\models A[e]$.
- Nech $e(x) = 0$. Potom formula $A' : \neg x = 0$ nie je splnená v ohodnotení e, t.j. $\mathcal{M} \not\models A'[e]$.

To ale znemaná, že formula A ani jej negácia A' nie sú splniteľné (a teda dokázateľné) v elementárnej aritmetike.

Poznámka 2.1.4 *(:* Vetu o dedukcii v predikátovej logike nemožno vysloviť pre ľubovoľnú formulu. Ukážeme to na nasledujúcom príklade: Majme formuly A, A'

$$A : \neg x = 0$$
$$A' : \neg y = 0$$

[1] v opačnom prípade implikácia triviálne platí

A' je inštancia formuly A. Potom ale platí:

$$A \vdash A' \quad \text{čiže}$$
$$\neg(x = 0) \vdash \neg(y = 0)$$

Môžem podľa vety o dedukcii napísať, že $\vdash \neg(x = 0) \to \neg(y = 0)$? Nie, pretože ak vezmeme ohodnotenie e nasledovne

$$e(x) = m, \quad m \neq 0$$
$$e(y) = 0$$

dostávame

$$\mathcal{M} \not\models (A \to A')[e]$$

Dôležitým faktom je, že pri dôkaze sme totiž skryte použili pravidlo zovšeobecnenia na voľnú premennú $\Rightarrow$ nemôžeme použiť VD. *:)*

Dôsledok: 2.1.1 (Vety o korektnosti) *Ak teória T v jazyku L má model $\mathcal{M}$, potom T je bezosporná.*

Dôkaz: Nech $\mathcal{M}$ je model T. Teória T je tým pádom bezosporná. Uvažujme ďalej, že A je ľubovoľná uzavretá formula jazyka L. Potom práve jedna z formúl A, $\neg A$ je pravdivá v modeli $\mathcal{M}$ (podľa Tarského definície splniteľnosti). Lenže tá, ktorá nie je pravdivá, nie je ani dokázateľná (podľa vety o korektnosti).
■

Tento výsledok hovorí, ze ak máme vyšetriť bezospornosť nejakej teórie, treba nájsť jej model. Dôkazy bezospornosti môžeme rozdeliť na 2 typy:

- syntaktické – sú to konečné posutpnosti symbolov, alebo formúl. Ak chceme dokázať bezospornosť T, môžeme popísať postup, ako dôkaz sporu v T prevedieme na dôkaz sporu v teórii S, o ktorej vieme, že je bezosporná. Napríklad ak T je predikátová logika, môžeme ju previesť na výrokovú logiku S.
- sémantické – niekedy nie je možné dokazovať syntakticky. Sémanticky dokazujeme tak, že nájdeme potenciálne nekonečný model $\mathcal{M}$ teórie T.

Príklad 2.1.5 (Bezospornosť predikátovej logiky) Ideme ukázať, že predikátová logika je bezosporná na základe toho, že výroková logika je bezosporná.

Máme jazyk L – jazyk prvého rádu, ktorý rozšírime o konštantu $c \notin L$. Dostaneme tak jazyk $L' = L \cup \{c\}$ zohrávajúci dôležitú rolu v dôkaze.

Proces dokazovania bude prebiehať nasledovne: Každý term formuly A nahradíme konštantou c, ďalej z danej formuly vynechávame všetky kvantifikátory a premenné bezprostredne spojené s kvantifikátorom.

Každej formule A na jazyku L teda priradíme formulu A^* na jazyku L' nasledovne:

1. A je tvaru $P(t_1, \ldots, t_n)$, tak $A^* : P(c, c, \ldots, c)$.[2]
2. A je tvaru $t_1 = t_2$, tak $A^* : c = c$.
3. A je tvaru $B \to C$, potom $A^* : B^* \to C^*$.
4. A je tvaru $B \,\square\, C$, potom $A^* : B^* \,\square\, C^*$.
5. A je tvaru $\neg B$, potom $A^* : \neg B^*$

[2] O funkčné symboly sa nemusíme starať – nahradili sme ich totiž konštntou c.

6. A je tvaru $(Qx)B$, potom $A^* : B^*$.

Ak jazyk L je jazyk bez rovnosti a $\vdash_L A$, potom o formule A^* tvrdíme, že je to tautológia. Na druhú stranu, ak L je jazyk s rovnosťou a $\vdash_L A$, potom A^* je tautologický dôsledok $c = c$.[3]

Teraz ukážeme, že predikátová logika nie je sporná: Tvrdíme, že pre žiadnu formulu A nie je $\vdash A$ aj $\vdash \neg A$. Ak by to platilo, dostali by sme sa do sporu, že vo výrokovej logike je $\vdash A^*$ aj $\vdash \neg A^*$.

2.2 Veta o úplnosti

Gödelova veta, ktorú si teraz vyslovíme a dokážeme, má 2 varianty.

Veta 2.2.1 (Gödel, 1. variant) *Nech T je teória v jazyku L a nech A je ľubovoľná formula jazyka L. Potom $T \vdash A \iff T \models A$, čiže A je dokázateľná práve vtedy keď je splnená v každom modeli teórie T.*

Veta 2.2.2 (Gödel, 2. variant) *Teória T je bezosporná práve vtedy, ked T má model.*

Poznámka 2.2.1 *(:* Varianta 1 Gödelovej vety vyplýva z variantu 2. *:)*

Dôkaz: [Poznámky] Veta o dedukcii mala nasledovný dôsledok:

Majme teóriu T a jej formulu A. Nech A' označuje uzáver formuly A. Potom platí: $T \vdash A \iff T \cup \{\neg A'\}$ je sporná teória.

V našom prípade z 2. varianty Gödelovej vety dostávame $T \vdash A \iff T \cup \{\neg A'\}$ nemá model. Toto znamená, že v každom modeli teórie T je pravdivý uzáver A'. Z toho dostávame $T \models A' \Rightarrow T \models A$ (ak zoberieme ľubovoľný model $\mathcal{M}$ teórie T, formula A' je v ňom splnená ale to nutne znamená, že aj formula A v ňom musí byť splnená) a teda z platnosti variantu 2 vyplýva variant 1.

■

Dôkaz: [2. variantu Gödelovej vety] Budeme sa snažiť zostrojiť model pre teóriu, ktorá je bezosporná. Majme bezospornú teóriu s jazykom L. Potrebujeme v prvom rade univerzum – M. K dispozícii máme len syntaktické prostriedky teórie. Preto ako kandidát na M prichádza do úvahy množina termov bez premenných. Tieto termy majú jednoznačnú realizáciu (sami sebe budú realizáciou).[4] V našom modeli budú teda všetky objekty teórie charakterizované termami.

Ďalšou otázkou je, ako definovať splniteľnosť. Malo by platiť, že formula je splniteľná práve vtedy keď je dokázateľná, čize

$$A[e] \iff T \vdash A$$

Pri konštrukcii modelu sa nám pritrafia isté nepríjemnosti, ktoré bude treba riešiť:

1. Jazyk L nemusí obsahovať žiadne konštanty (a teda žiadne termy bez premenných).

2. Ak jazyk L bude jazyk s rovnosťou, môže sa stať, že v teórii T bude $T \vdash t = s$, ale t a s sú rôzne termy bez premenných (rôzne konštanty).

3. Nech $\mathcal{M}$ je ľubovoľná realizácia jazyka L a A je uzavretá formula jazyka L. Potom práve jedna z formúl A, $\neg A$ je pravdivá, ale žiadna z nich nemusí byť dokázateľná v T.

[3] Toto sa na prvý pohľad zá byť kontraintuitívne. Majme totiž formulu $\exists x \exists y \neg(x = y)$. Z jej dokázateľnosti tvrdíme dokázateľnosť $\neg(c = c)$ čo je evidentne nepravda.

Problém je v tom, že $\exists x \exists y \neg(x = y)$ dokázateľná nie je. Prečo? Pozrime sa na celú našu redukciu. Akoby sme dosadili špeciálny model $\mathcal{M}$, ktorého univerzum M tvorí iba jediná hodnota – konštanta c. Teda, ak pôvodná formula bola dokázateľná $\Rightarrow$ platí v každom modeli, teda špeciálne aj našom. Lenže v našom modeli sa interpretuje ako $\neg(c = c)$ a teda nemohla byť dokázateľná.

[4] Pre ujasnenie tejto myšlienky odporúčame čitateľovi nalistovať si kapitolu o Herbrandovských interpretáciach a nahliadnuť tak pointu tohoto činu.

4. Môže sa stať, že uzavretá formula $(\exists x)B$ je dokázateľná v teórii T, ale pre žiaden term t bez premenných formula $B_x[t]$ nie je dokázateľná v T. To znamená, že podľa Tarského definície pravdivosti je $(\exists x)B$ nepravdivá, čo je spor s vetou o korektnosti.

Ako odstránime tieto nedostatky? Odstránenie bodu 2 je jednoduché – riešime vhodnou faktorizáciou, čiže zavedieme si množinu τ, čo je množina všetkých termov bez premenných a na nej zavedieme reláciu ekvivalencie.

Body č. 1, 3 a 4 sa riešia tzv. úplným konzervatívnym rozšírením teórie (Henkinovským). Budú to tzv. konzervatívne teórie (na pôvodnom jazyku nezískame žiadne nové teorémy a ani nestratíme žiadne). Nachvíľu teda opustíme dôkaz Gödelovej vety, aby sme si mohli niečo porozprávať o Henkinovej teórii. K dôkazu sa vrátime, keď na to budeme mať pripravenú pôdu.
■

Definícia 2.2.1 (Úplná teória) *Hovoríme, že teória T s jazykom L je úplná, ak T je bezosporná teória a pre ľubovoľnú* `uzavretú` *formulu A na jazyku L platí, že buď A alebo $\neg A$ je dokázateľná v T.*

Poznámka 2.2.2 *(:* Pojem úplnosti teda zodpovedá nasledujúcej konštrukcii: Majme teóriu T nad jazykom L a jej model $\mathcal{M}$. Model $\mathcal{M}$ rozhoduje o pravdivosti každej uzavretej formuly. Označme ako $T_h(\mathcal{M})$ množinu všetkých pravdivých uzavretých formúl T. Potom platí, že $T_h(\mathcal{M})$ je úplná.

Je dôležité si uvedomiť, že neberieme otvorené formuly – napr. formula $x = 0$ v elementárnej aritmetike nemusí byť pradivá, pretože závisí od ohodnotenia x. *:)*

Poznámka 2.2.3 *(:* V úplnej teórii (a teda špeciálne v T_h) nemôže nastať problém 3, ktorý sme spomínali. *:)*

Definícia 2.2.2 (Henkinova teória) *Hovoríme, že teória T s jazykom L je Henkinova, ak pre ľubovoľnú uzavretú formulu $(\exists x)B$ jazyka L platí*

$$T \vdash (\exists x)B \to B_x[c]$$

pre nejakú konštantu c.

Poznámka 2.2.4 *(:* Ak je teória Henkinova, tak sme vyriešili problémy 1, 4. *:)*

Lema 2.2.1 *Ak T je úplná a Henkinova teória, tak potom T má model.*

Dôkaz: Nech L je jazyk teórie T a nech τ je množina všetkých termov jazyka L bez premenných. Na množine τ definujeme reláciu ekvivalencie nasledovne:

$$\forall t_1, t_2 \in \tau : t_1 \equiv t_2 \iff T \vdash t_1 = t_2$$

Rovnosť je reflexívna, symetrická, tranzitívna, teda týmto spôsobom definovaná relácia je relácia ekvivalencie a rozdeľuje nám množinu τ na triedy ekvivalencie:

$$[t] = \{s \in \tau | t \equiv s\}$$

Týmto sme vyriešili problém 2.

Zadefinujme si univerzum M tak, že ho budú tvoriť vyššie popísané triedy ekvivalencie. Nech f je ľubovoľný n-árny funkčný symbol a nech $[t_1], [t_2], \ldots, [t_n] \in M$. Definujeme funkciu f v relačnej štruktúre $\mathcal{M}$ nasledovne:

$$f_{\mathcal{M}}([t_1], \ldots, [t_n]) = [f(t_1, \ldots t_n)]$$

Bolo by potrebné ukázať, že táto definícia je konzistentná. Teda, že platí $f_{\mathcal{M}}([t_1], \ldots, [t_n]) = f_{\mathcal{M}}([s_1], \ldots, [s_n])$ za predpokladu $\forall i \in 1, \ldots, n : s_i \equiv t_i$. Inak povedané, nesmie záležať na výbere reprezentantov. Taktiež je dobré si uvedomiť, že $[t_{x_1,\ldots,x_n}[t_1, \ldots, t_n]] = t[e]$, ak platí $e(x_i/t_i)$ resp. $e(x_i) = t_i$.

Podobne, nech P je n-árny predikátový symbol rôzny od '=' (predikát '=' sme si už zaviedli). V tom prípade definujeme

$$([t_1], \ldots, [t_n]) \in P_{\mathcal{M}} \iff T \vdash P(t_1, \ldots, t_n)$$

Zostáva nám ukázať, že nami definované $\mathcal{M}$ je naozaj modelom teórie T, čo bude predmetom nasledujúcej vety.
■

Veta 2.2.3 (O kanonickej štruktúre) *Nech T je úplná Henkinovská teória a nech $\mathcal{M}$ je definované podľa dôkazu lemy 2.2.1. Potom $T \vdash A \iff \mathcal{M} \models A$.*

Dôkaz: Budeme postupovať matematickou indukciou vzhľadom na zložitosť formuly. Pri dokazovaní sa ale obmedzíme iba na uzavreté formuly.

1: Báza indukcie:

- Formula A je tvaru $P(t_1, \ldots, t_n)$. Pritom $t_1, \ldots t_n$ sú termy bez premenných (inak by formula A nebola uzavretá). Podľa definície splniteľnosti platí, že A je pravdivá v T práve vtedy keď je dokázateľná v T. Zoberme si teraz ohodnotenie e také, že $t_i[e] = t_i$ (Čiže každý term realizujeme samým sebou). Podľa definície je uzavretá formula A pravdivá práve vtedy, keď je splnená aspoň pre jedno ohodnotenie e (vtedy je automaticky splnená pre všetky ohodnotenia e). Teda

$$\begin{aligned} \mathcal{M} \models A &\iff \mathcal{M} \models A[e] \\ &\iff (t_1[e], t_2[e], \ldots, t_n[e]) \in P_{\mathcal{M}} \\ &\iff ([t_1], [t_2], \ldots, [t_n]) \in P_{\mathcal{M}} \\ &\iff T \vdash P(t_1, t_2, \ldots, t_n) \equiv A \end{aligned}$$

- Formula môže byť tvaru $A : t_1 = t_2$. V tom prípade $\mathcal{M} \models t_1 = t_2 \iff [t_1] = [t_2] \iff T \vdash t_1 = t_2$

2: Indukčný krok:
Máme niekoľko možností, ako mohla formula A vzniknúť:

- $A : \neg B$. Na formulu B sa vzťahuje IP, keďže B je uzavretá formula. Teda $\mathcal{M} \models A \iff \mathcal{M} \not\models B$. Vieme, že teória T je úplná, že buď $T \vdash A$ alebo $T \vdash B$. Keďže je bezosporná, platí práve jedna možnosť. Tým sme ale ukázali, že $\mathcal{M} \models A \iff T \vdash A$.
- $A : B \to C$. Na formuly B, C sa vzťahuje IP. Rozoberme si obe implikácie tvrdenia $\mathcal{M} \models B \to C \iff T \vdash B \to C$.

  $\Rightarrow$: Vieme, že $(B \to C) \leftrightarrow \neg B \vee C$. Čiže môžeme predpokladať, že aspoň 1 z tvrdení $\mathcal{M} \models \neg B$, $\mathcal{M} \models C$ platí. Rozoberme obe možnosti – pri prvej predpokladáme, že $\neg B$ je pravdivá (a z IP dokázateľná[5]):
  - $T \vdash \neg B$ – IP
  - $\vdash \neg B \to (B \to C)$ – z vety o neutrálnej formule
  - $T \vdash B \to C$ – MP na prvé 2 formuly

  V druhom prípade predpokladáme pravdivosť C, t.j.
  - $T \vdash C$ – IP
  - $\vdash C \to (B \to C)$ – A1
  - $T \vdash B \to C$ – MP

  Záver: ak platí $\mathcal{M} \models B \to C$, tak je formula $B \to C$ dokázateľná v T.

[5]Presnejšie povedané, IP nestačí, potrebujeme spraviť ešte ďalší krok kvôli negácii. Ten sme už ale rozobrali.

$\Leftarrow$: Uvažujeme, že $T \vdash B \to C$. Teória T je úplná teória a $B \to C$ je uzavretá. Pre každú uzavretú formulu platí jedna z možností $T \vdash \neg B$ (potom $\mathcal{M} \models \neg B$ a sme hotoví) alebo $T \vdash B$. Vtedy ale musí platiť $T \vdash C$ a teda $\mathcal{M} \models C$. Tým je tvrdenie dokázané.

Ešte sa môžeme vrátiť k tomu, prečo platí $T \vdash C$. Uvažujme totiž $T \vdash \neg C$.

- $T \vdash B \to C$
- $T \vdash B$ – predpoklad
- $T \vdash C$ – MP
- $T \vdash \neg C$ – predpoklad a zároveň spor s bezospornosťou teórie T.

– $A : (\forall x)B$. Pre každú inštanciu formuly B tvrdenie platí. Pretože je teória úplná, môžu nastať 2 prípady:

* Platí $T \vdash A$. Teda, $T \vdash (\forall x)B$. Ďalej platí pre ľubovoľnú konštantu c, že je dokázateľné $\vdash (\forall x)B \to B_x[c]$ – axióma špecifikácie. Potom aj $T \vdash B_x[c]$ (MP na axiómu špecifikácie). Lenže z IP dostávame $\forall c : \mathcal{M} \models B_x[c] \Rightarrow \mathcal{M} \models (\forall x)B$.
* Platí $T \vdash \neg A$. Vtedy $T \vdash (\exists x)\neg B$. Ďalej, keďže teória je Henkinovská, platí tiež $T \vdash (\exists x)\neg B \to \neg B_x[c]$. Pomocou MP odvodíme $T \vdash \neg B_x[c]$. Podobne ako v predchádzajúcom prípade máme $\mathcal{M} \models \neg B_x[c] \Rightarrow \mathcal{M} \not\models A$ (formula $B_x[c]$ je nepravdivá a preto aj formula $(\forall x)B$ je nepravdivá). Nuž ale potom $\mathcal{M} \models \neg A$.

Ukázali sme, že pre uzavreté formuly vieme pomocou indukcie dokázať tvrdenie vety. Teraz, nech A je ľubovoľná formula z teórie T. Pre ňu platí, že $T \vdash A$ (predpoklad). Potrebujem dokázať, že $T \vdash A \iff \mathcal{M} \models A$. Zoberiem si A' – uzáver formuly A. Na A' sa vzťahuje naša indukcia a teda $\mathcal{M} \models A' \iff T \vdash A'$. Podľa vety o uzávere ale platí $\mathcal{M} \models A \iff \mathcal{M} \models A'$ čo je $\iff T \vdash A'$ a z vety o uzávere $\iff T \vdash A$.

■

Záver: Pre ľubovoľnú teóriu, ktorá je idealizovaná (Henkinova a úplná), vieme zostrojiť model.

2.3 Rozšírenia teórie

V nasledujúcej časti budeme definovať rozšírenia, ktoré v istom zmysle ani nepomôžu ani neuberú sile teórii.

Definícia 2.3.1 (Rozšírenie jazyka) *Jazyk L' je rozšírením jazyka L, ak každý špeciálny symbol jazyka L (prípadne aj symbol "=") je v jazyku L' obsiahnutý s rovnakým významom a s rovnakou árnosťou.*

Príklad 2.3.1 Nech jazyk L' je jazyk s rovnosťou a špeciálnymi symbolmi "$<$" a "0". Jazyk L má symboly "$<$" a "=". Jazyk L' je potom rozšírením jazyka L.

Definícia 2.3.2 (Rozšírenie teórie) *Majme teóriu T' s jazykom L'. Hovoríme, že T' je rozšírením teórie T s jazykom L, ak platí, že L' je rozšírením jazyka L a pre každý formulu A jazyku L platí $T \vdash A \Rightarrow T' \vdash A$.*

Príklad 2.3.2 Uvažujme teóriu grúp – je to teória s rovnosťou, ktorá používa špeciálny symbol "+" a existuje v nej neutrálny prvok "0".

Axiómy tejto teórie sú:

- $\forall x, y, z : (x + y) + z = x + (y + z)$
- $(x + 0) = x = (0 + x)$
- $(x + (-x)) = 0 = ((-x) + x)$

Ak si vezmeme relačnú štruktúru $\mathcal{M} = \langle \mathbb{N}_0, 0, +, - \rangle$, táto realizuje jazyk teórie grúp. Nie je však jej modelom (lebo nie všetky axiómy sú splnené, menovite napríklad inverzné prvky). Pokiaľ ale vezmeme $\mathcal{M} = \langle \mathbb{Z}, 0, +, - \rangle$, táto množina je realizáciou a zároveň aj modelom teórie grúp.

Teraz si zoberme jazyk $L = \{0, 1, +, -, *, ^{-1}\}$ a uvažujme postupne nasledujúce teórie:

1. teória grúp
2. teória okruhov
3. teória oborov integrity
4. teória telies
5. teória polí
6. teória zväzov

Každá z týchto teórii je rozšírením tej predchádzajúcej.

Poznámka 2.3.1 *(:* Je dôležité si uvedomiť, že nie všetky axiómy pôvodnej teórie T sa musia nachádzať aj v rozšírenej teórii T' – stačí, ak sa dajú odvodiť v T'. *:)*

Poznámka 2.3.2 *(:* Ak teória T' nad jazykom L' je rozšírením teórie T nad jazykom L a vieme že T' je bezosporná, potom aj T je bezosporná. *:)*

Dôkaz: Predpokladajme, že T je sporná teória. Teda je v nej dokázateľná každá formula. Špeciálne, je dokázateľné $T \vdash A$ a $T \vdash \neg A$. Keďže T' je rozšírenie, musí potom platiť $T' \vdash A$ a $T' \vdash \neg A$. To je ale spor.
■

Definícia 2.3.3 (Konzervatívne rozšírenie) *Hovoríme, že teória T' nad jazykom L' je konzervatívnym rozšírením teórie T nad jazykom L, ak pre každú formulu A nad jazykom L platí $T' \vdash A \Rightarrow T \vdash A$. Inak povedané, konzervatívnym rozšírením nezískame žiadne nové teorémy.*

Poznámka 2.3.3 *(:* Spojením posledných dvoch definícii dostávame, že pre konzervatívne rozšírenie T', L' teórie T, L platí

$$\forall A \in L: \qquad T \vdash A \iff T' \vdash A$$

:)

Poznámka 2.3.4 *(:* Nech T', L' je konzervatívne rozšírenie T, L. Potom platí (z predchádzajúcej poznámky) T je bezosporná $\iff$ T' je bezosporná. *:)*

Veta 2.3.1 (Henkinova) *K ľubovoľnej teórii T môžeme zostrojiť Henkinovu teóriu T_H, ktorá je konzervatívnym rozšírením teórie T.*

Dôkaz: Teóriu T rozšírime a priradíme k nej teóriu T_H tak, že jednak rozšírime jazyk teórie a jednak pridáme axiómy. Nech teória T má jazyk L. Budeme tvoriť rozšírený jazyk L_H tak, že budeme pridávať konštanty:

Pre každú formulu A napísanú v jazyku L, ktorá má jedinú *voľnú* premennú x vytvoríme konštanty $c_A, c_{\neg A}$ a nasledovné axiomy:

H1: $(\exists x)A \to A_x[c_A]$

H2: $A_x[c_{\neg A}] \to (\forall x)A$

Stačil by nám aj jeden typ axiómy, ako sa môžeme ľahko presvedčiť:

- $(\exists x)\neg A \to \neg A_x[c_{\neg A}]$ – H1

- $\neg\neg A_x[c_{\neg A}] \to (\forall x)\neg\neg A$ – obmena implikácie
- $A_x[c_{\neg A}] \to (\forall x)A$ – odstránenie dvojitej negácie

Konštanty $c_A, c_{\neg A}$ nazývame henkinovské konštanty prvého rádu. Tieto konštanty nám vytvoria množinu konštánt, označme ju C_1. Týmito konštantami rozšírime jazyk L.

Teraz zoberme formulu B na jazyku $L(C_1)$, ktorá obsahuje práve jednu voľnú premennú a aspoň jednu konštantu z C_1. K tejto formule priradíme podobne ako minule konštanty $c_B, c_{\neg B}$. Takto dosiahnuté konštanty budeme nazývať Henkinovské konštanty druhého rádu a ich množinu označíme ako C_2.

Induktívne pokračujeme ďalej a podobne vytvárame množiny $C_3, C_4, \ldots$ Množinu C_{n+1} vo všeobecnosti vytvoríme z množiny C_n, tak, že zoberieme formuly nad jazykom $L(C_n)$, ktoré obsahujú jednu voľnú premennú a aspoň jednu konštantu n-tého rádu.

Označme si teraz

$$L(C) = L \cup \bigcup_{i=1}^{\infty} C_i$$

Teóriu T_H bude tvoriť rozšírenie $L(C)$ jazyka L, axiómy budú axiómy T ku ktorým pridáme všetky axiómy $H1$. Je ihneď zrejmé, že T_H je rozšírenie teórie T. Potrebujeme ukázať, že T_H je konzervatívne rozšírenie teórie T, t.j. že pre každú formulu A jazyka L platí $T_H \vdash A \Rightarrow T \vdash A$.

Poďme to dokázať:

- Nech platí, že v T_H je dokázateľná formula A a nech $B_1, B_2, \ldots, B_n$ sú všetky Henkinovské axiómy vyskytujúce sa v dôkaze A. Keďže dôkaz je konečný, týchto axióm je konečný počet. Ďalej môžeme uvažovať (ako sme už ukázali), že všetky axiómy $B_1, \ldots, B_n$ sú typu $H1$. Máme teda
$$T, B_1, \ldots, B_n \vdash A$$
- Keďže axiómy $B_1, \ldots, B_n$ sú uzavreté formuly, môžeme použiť vetu o dedukcii a dostávame
$$T \vdash B_1 \to B_2 \to \ldots \to B_n \to A$$
- Axiómy navyše môžeme poprehadzovať tak, aby B_1 obsahovala konštantu maximálneho rádu. Tvrdíme, že táto konštanta sa určite nenachádza v A (pretože je nad pôvodným jazykom L) a ani v ostatných B_i (pretože všetky axiómy B_i rovnakého rádu majú svoju "hlavnú" konštantu inú). Teda B_1 je tvaru $(\exists x)D \to D_x[c_D]$, pričom c_D nie je je použitá v $A, B_2, B_3, \ldots, B_n$.
$$T \vdash ((\exists x)D \to D_x[c_D]) \to [B_2 \to \ldots \to B_n \to A]$$
- Použijeme vetu o konštantách a dostávame
$$T \vdash ((\exists x)D \to D_x[w]) \to [B_2 \to \ldots \to B_n \to A]$$
kde w je nová premenná.
- Teraz môžeme použiť pravidlo zavedenia existenčného kvantifikátora – ak je dokázateľné $T \vdash A \to B$ a w nie je voľná v B, potom je dokázateľné aj $T \vdash (\exists w)A \to B$. Čiže
$$T \vdash (\exists w)((\exists x)D \to D_x[w]) \to [B_2 \to \ldots \to B_n \to A]$$
- Ďalej použijeme prenexnú operáciu $(Qx)(A \to B) \iff (A \to (Qx)B)$ (za predpokladu, že x nie je voľná v A), aby sme w preniesli dovnútra. Výsledkom je
$$T \vdash ((\exists x)D \to (\exists w)D_x[w]) \to [B_2 \to \ldots \to B_n \to A]$$

- Z vety o variantoch ale vieme, že platí (pretože $(\exists w)D_x[w]$ je variant $(\exists x)D$) formula

$$T \vdash (\exists x)D \to (\exists w)D_x[w]$$

- A teda pomocou pravidla modus ponens získame

$$T \vdash B_2 \to B_3 \to \ldots \to B_n \to A$$

Opakovaním postupu ďalších $n-1$ krát dostaneme $T \vdash A$. Ukázali sme teda, že T_H s jazykom $L(C)$ je konzervatívne rozšírenie jazyka L.
■

Veta 2.3.2 (Lindenbaum) *Ak T je bezosporná teória s jazykom L, potom existuje úplné rozšírenie T' teórie T s rovnakým jazykom L.*

Dôkaz: Nech $\mathscr{S}$ je množina všetkých uzavretých formúl jazyka L. Ďalej definujeme množinu (podmnožín $\mathscr{S}$) $\mathcal{B} = \{S \mid S \subseteq \mathscr{S}, T \cup S \text{ je bezosporná}\}$. Množina $\mathcal{B}$ je čiastočne usporiadaná vzhľadom na inklúziu a (ako si neskôr ukážeme) má takzvanú konečnú vlastnosť – keď zoberieme ľubovoľnú podmnožinu $S \subseteq \mathscr{S}$, bude platiť

$$S \in \mathcal{B} \iff \forall \text{ konečné } S' \in \mathcal{B} : S' \subseteq S$$

Potrebujeme ukázať, že operácia inklúzie $\Psi, \Psi \subseteq \mathcal{B} \times \mathcal{B}$ je čiastočné usporiadanie, čiže je

- reflexívna

$$\forall S \in \mathcal{B} : (S, S) \in \Psi, \quad \text{t.j.}$$
$$S \subseteq S$$

- antisymetrická

$$(S_1, S_2) \in \Psi \wedge (S_2, S_1) \in \Psi \Rightarrow S_1 = S_2, \quad \text{t.j.}$$
$$S_1 \subseteq S_2 \wedge S_2 \subseteq S_1 \Rightarrow S_1 = S_2$$

- tranzitívna (dokážeme analogicky)

$\mathcal{B}$ je teda čiastočne usporiadaná inklúziou Ψ. Navyše

$$\emptyset \in \mathcal{B}, \text{ lebo } T \cup \emptyset = T$$

Ak by totiž $\emptyset$ nebola v $\mathcal{B}$, potom by T bola sporná.
Teraz ukážeme, že množina $\mathcal{B}$ má konečnú vlastnosť, čiže platí: Nech $S \in \mathscr{S}$, potom

$$S \in \mathcal{B} \iff \forall \text{ konečnú podmnožinu } S' \subseteq S \text{ platí } T \cup S' \text{ je bezosporná (teda } S' \in \mathcal{B})$$

$\Rightarrow$: Nech $S \in \mathcal{B}$. Potom $T \cup S$ je bezosporná. Ak teda $S' \subseteq S$ a S' je konečná, teória $T \cup S'$ bude tiež bezosporná $\Rightarrow S' \in \mathcal{B}$

$\Leftarrow$: Predpokladajme, že pre každú konečnú podmnožinu $S' \subseteq S$ je $T \cup S'$ je bezosporná. Chceme ukázať $S' \in \mathcal{B} \Rightarrow S \in \mathcal{B}$.

Tvrdenie dokážeme sporom. Predpokladajme, že $S \notin B$. Potom $T \cup S$ je sporná, čiže pre ľubovoľnú dokázateľnú formulu A je dokázateľné $\neg(A \to A)$.

Nech $A_1, A_2, \ldots, A_n$ je dôkaz platnosti $\vdash \neg(A \to A)$. Nech $B_1, B_2, \ldots, B_m$ sú tie formuly, ktoré sa v tom dôkaze vyskytujú a patria do množiny S. Tvrdíme, že ich počet $m \geq 1$. Prečo? Inak by bola priamo T sporná. Zoberme teraz ale konečnú množinu $S' = \{B_1, \ldots, B_m\}$. Zjavne $T \cup S'$ je sporná teória. To je ale spor s predpokladmi.

Teraz nachvíľu opustíme dôkaz Lindenbaumovej vety, aby sme sformulovali princíp maximality, ktorý sa nám bude hodiť.
■

Lema 2.3.1 (Princíp maximality) *Každá neprázdna podmnožina potenčnej množiny $\mathcal{P}(\mathscr{S})$ s konečnou vlastnosťou má maximálny prvok vzhľadom na inklúziu.*

Dôkaz: [Pokračovanie dôkazu Lindenbaumovej vety] Dostali sme sa do štádia, keď sme ukázali, že $\mathcal{B}$ má konečnú vlastnosť. Budeme teda pokračovať tým, že vytvoríme rozšírenie pôvodnej teórie nad rovnakým jazykom.

Nech S_0 je maximálny prvok množiny $\mathcal{B}$ vzhľadom na inklúziu, podľa princípu maximality existuje. Položme rozšírenie $T' = T \cup S_0$. Ukážeme, že T' je úplná teória, t.j. že pre ľubovoľnú uzavretú formulu A je dokázateľná v teórii T' buď A alebo $\neg A$.

Uvažujme sporom: nech T' nie je úplná teória. Potom existuje uzavretá formula A taká, že $T' \nvdash A$ a $T' \nvdash \neg A$. Lenže z tohoto je evidentné (keďže T' je bezosporná), že aj $T'' = T' \cup \{\neg A\}$ je bezosporná teória.[6] To je ale v spore s tým, že S_0 je maximálny prvok $\mathcal{B}$.

Dosiahli sme zúplnenie teórie. Pre teóriu T sme získali T', ktorá je bezosporná a je úplným rozšírením T na rovnakom jazyku.
■

Zhrňme si, čo sme doteraz dosiahli: Keď máme teóriu T nad jazykom L, vieme ju rozšíriť na henkinovskú teóriu T_H s jazykom $L(C)$. V prípade, že T je bezosporná, bude aj T_H bezosporná. Podľa Lindenbaumovej vety dokážem vytvoriť teóriu T'_H s jazykom $L(C)$, ktorá je úplná a má model $\mathcal{M}'$. Našim cieľom je teraz získať model $\mathcal{M}$ pre pôvodnú teóriu.

Definícia 2.3.4 (Redukcia) *Majme teóriu T nad jazykom L a jej rozšírenie T', L'. Nech $\mathcal{M}'$ je realizácia jazyka L'. Redukovaním štruktúry $\mathcal{M}'$ na jazyk L získame realizáziu teórie T v jazyku L. Formálne redukciu definujeme nasledovne:*

- *Univerzum $\mathcal{M}$ bude to isté univerzum ako univerzum $\mathcal{M}'$.*
- *$\mathcal{M}$ obsahuje iba také relácie a zobrazenia, ktoré realizujú špecálne symboly jazyka L v realizácii $\mathcal{M}'$. Teda, ak f je ľubovoľný n-ány funkčný symbol jazyka L a $f_{\mathcal{M}'}$ je zobrazenie, ktoré realizuje f v $\mathcal{M}'$, potom zostáva realizáciou f v $\mathcal{M}$. Podobne to bude aj s n-árnym predikátom P.*

Budeme hovoriť, že $\mathcal{M}$ vzniklo redukciou $\mathcal{M}'$ na jazyk L a zapisovať $\mathcal{M} = \mathcal{M}' \triangle L$.[7] *Alebo opačne, $\mathcal{M}'$ je expanzia realizácie $\mathcal{M}$.*

Poznámka 2.3.5 *(:* Nech $\mathcal{M}$ je redukcia $\mathcal{M}'$ na jazyk L a nech A je formula jazyka L. Potom platí $\mathcal{M} \models A \iff \mathcal{M}' \models A$. *:)*

Dôkaz: Máme teda tvrdenie $\mathcal{M} \models A$, t.j. pre ľubovoľné ohodnotenie v relačnej štruktúre $\mathcal{M}$ je formula A pravdivá. Podobne je to aj s $\mathcal{M}' \models A$. Všimnime si, že univerzum je to isté. Nuž ale potom aj ohodnotenia premenných musia byť rovnaké. Čo sa týka realizácie $\mathcal{M}, \mathcal{M}'$, tak hodnota formuly A závisí od realizácie špeciálnych symbolov jazyka L. Tie sa ale podľa definície realizujú rovnako. Záverom teda je, že pre formulu A su realizácie $\mathcal{M}, \mathcal{M}'$ rovnaké a teda platí tvrdenie poznámky.
■

Veta 2.3.3 *Nech T' je rozšírenie teórie T s jazykom L. Ak $\mathcal{M}'$ je model T' a $\mathcal{M} = \mathcal{M}' \triangle L$, tak $\mathcal{M}$ je model T.*

[6] Odvoláme sa na dôsledok vety o dedukcii dokázaný niekedy v Úvode do matematickej logiky: ak A je uzavretá, potom $T \vdash A \iff T \cup \{\neg A'\}$ je sporná teória.

[7] Na prednáške bolo miesto $\triangle$ použíté niečo ako $\wedge$, len ľavá nožička bola dlhšia ako pravá.

Dôkaz: Nech $A \in T$. Teda, $T \vdash A$. Potom (pretože T' je rozšírenie T) platí $T' \vdash A$. Čiže z vety o korektnosti dostávame $\mathcal{M}' \models A$. Ale A je nad jazykom L a platí $\mathcal{M} = \mathcal{M}' \triangle L$. Teda, z predchádzajúcej poznámky vyplýva $\mathcal{M} \models A$.
■

Rozpamätajme sa na náš pôvodný zámer, načo sme sa vlastne zaoberali rozšíreniami – bola to práve Gödelova veta.

Dôkaz: [Dokončenie 2. variantu Gödelovej vety] Naším zámerom bolo zostrojiť model pre teóriu, ktorá je bezosporná. Postupujme teda nasledovne: K teórii T existuje henkinovské rozšírenie T_H, ktoré sa dá (konzervatívne) rozšíriť podľa Lindenbaumovej vety na úplnú teóriu T'_H. O tejto teórii vieme, že je bezosporná a teda vieme podľa vety o kanonickej štruktúre zostrojiť jej model $\mathcal{M}'$. Nuž a teraz nám stačí redukovať $\mathcal{M}'$ na pôvodný jazyk L a dostávame $\mathcal{M} = \mathcal{M}' \triangle L$ – model pôvodnej teórie T. Naopak, ak k teórii T existoval model, zrejme sa nemôže stať, že by bola sporná. Tým sme dokázali 2. variant Gödelovej vety.
■

2.4 Veta o kompaktnosti

Veta 2.4.1 (O kompaktnosti) *Nech T je množina formúl jazyka L, A je formula L. Potom $T \models A \iff \exists$ konečná podmnožina $T' \subseteq T : T' \models A$.*

Dôkaz: Podľa Gödelovej vety o úplnosti v predikátovej logike platí $T \models A \iff T \vdash A$. Nech $A_1, A_2, \ldots, A_n$ je konečná postupnosť formúl – dôkaz A. Zoberme $T' = \{B_1, B_2, \ldots, B_m\}$, kde B_i sú axiómy T nachádzajúce sa v dôkaze A.

Potom môžeme písať $T' \vdash A \iff T' \models A$.
■

Príklad 2.4.1 Na základe vety o kompaktnosti ukážeme, že teóriu telies charakteristiky 0 nedokážeme v teórii prvého rádu zapísať pomocou konečného počtu axióm.

Nech T je teória telies charakteristiky 0 (s rovnosťou) a jazykom $L = \{0, 1, +, *\}$. Označme si pre $p \in N, p \geq 1$ výraz $p \times 1$ ako

$$p \times 1 \equiv \underbrace{1 + (1 + (1 + \ldots (1 + 1)\ldots)}_{p}$$

Ďalej si označme formulu P_p ako $P_p : p \times 1 = 0$. Pre telesá charakteristiky p platí (z definície charakteristiky)

$$\models \neg P_1 \wedge \neg P_2 \wedge \cdots \wedge \neg P_{p-1} \wedge P_p$$

Ak teleso nemá konečnú charaktetistiku, tak jeho charakteristika je 0.

Uvažujme formulu A teórie telies charakteristiky 0. Pre A platí

$$T \models A \iff T' \subseteq T, T' \text{ konečná}$$

Teória T' obsahuje len konečne veľa axióm $\neg P_p$. Označme m najväčší index axiomy, ktorá patrí do T'. Potom formula A je splnená aj vo všetkých telesách dostatočne veľkej konečnej charakteristiky (presnejšie povedané charakteristiky $> m$). Ak teda formula A je teorémou telies charakteristiky 0, tak platí aj vo všetkých telesách dostatočne veľkej charakteristiky. Toto začína napovedať, že čosi nie je na kostolnom poriadku. Dotiahnime teda naše argumenty do konca.

Uvažujme teraz axiómy $A_1, \ldots A_n$ teórie telies s charakteristikou 0.

$$T' \models A_i \rightarrow T' \models A_1 \wedge A_2 \wedge \cdots \wedge A_n \equiv B$$

Formula B teda platí vo všetkých telesách charakteristiky 0. Lenže ako sme už povedali, tým pádom platí aj vo všetkých telesách dostatočnej charakteristiky. To je ale spor, pretože axiómy telies charakteristiky 0 nemôžu platiť v telesách konečnej charakteristiky.

Záverom teda je, že logikou prvého rádu nemôžeme konečným počtom axiom charakterizovať teóriu telies. V logike prvého rádu totiž kvantifikujeme len individuá.

Poznámka 2.4.1 *(:* Ak zavedieme ďalší druh premenných, prirodzené čísla, nekonečne veľa axiom typu $\neg P_p$ môžeme nahradiť jednou formulou:

$$(\forall p)(p \times 1 \neq 0)$$

Toto sa v literatúre terminologicky nazýva `slabá logika druhého rádu`. V nej vieme konečne axiomatizovať teóriu telies charakteristiky 0. Tým pádom `v slabej logike druhého rádu neplatí veta o kompaktnosti`. *:)*

Poznámka 2.4.2 *(:* Poznáme doteraz tieto logiky:

- logika 1. rádu – premenné len pre indivíduá
- logika 2. rádu – premenné pre množiny indivíduí
- slabá logika 2. rádu – premenné pre indivíduá a prirodzené čísla

:)

Mali sme Godelovu vetu v dvoch tvaroch. Prvý bol $T \models A \iff T \vdash A$, druhý variant znel "Teória je bezosporná, keď má model". Preto aj veta o kompaktnosti bude mať druhý tvar.

Veta 2.4.2 (2. tvar vety o kompaktnosti) *Nech T je množina formúl jazyka L. Model teórie T existuje práve vtedy, keď každá konečná podmnožina $T' \subseteq T$ má model.*

Dôkaz: Z 2. Gödelovej vety vyplýva, že T má model $\iff$ je bezosporná. Z lindenbauma zase, že T je bezosporná $\iff$ každá konečná $T' \subseteq T$ je bezosporná, čo opäť z Gödelovou vety $\iff$ každá konečná podmnožina $T' \subseteq T$ má model.
■

Príklad 2.4.2 Pomocou vety o kompaktnosti tohto tvaru dokážeme zaručiť, že pre Peanovu aritmetiku existujú aj neštandardné modely. Zopakujme si najskôr jej axiómy:

1. $\vdash \neg(S(x) = 0)$
2. $\vdash (S(x) = S(y)) \to (x = y)$
3. $\vdash (x + 0) = x$
4. $\vdash (x + S(y)) = S(x + y)$
5. $\vdash (x * 0) = 0$
6. $\vdash (x * S(y)) = ((x * y) + x)$

   Doteraz sme dostali Robinsonovu aritmetiku. Peanovu aritmetiku dostávame pridaním axiómy indukcie:

7. $\vdash A_x[0] \to (\forall x)\Big(A \to (A_x[S(x)] \to (\forall x)A)\Big)$

Táto aritmetika má model $\mathcal{N} = \langle 0, 1, S, +, *, \mathbb{N}_0 \rangle$.

Ukážeme, že Peanova aritmetika má aj neštandardné modely. Definujme množinu "numerálov" $\bar{n}$ pre $n \in \mathbb{N}_0$ ako termoy jazyka L nasledovne:[8]

- $\bar{0} = 0$
- $\overline{n+1} = S(\bar{n}) = \underbrace{S(S(\cdots S}_{(n+1)\text{-krát}}(0)\cdots))$

[8] Veľmi podobne ako Herbrandovské interpretácie, viď príslušnú kapitolu

K jazyku L zostrojíme rozšírený jazyk L_c tak, že do L pridáme konštantu c a teóriu rozšírime o axiómy

$$\vdash C_n : c \neq \bar{n} \qquad \forall n \in \mathbb{N}_0$$

Vidíme, že každá konečná podmnožina T_c má model, ktorý vznikne expanziou štandardného modelu $\mathcal{N}$. Konštantu c budeme jednoducho realizovať ako indivíduom n, ktoré nepatrí do indivíduí použitých v axiómach (a teda je istým spôsobom "nové"). Čiže každá $T' \subseteq T_c$ má model a na základe vety o kompaktnosti aj T_c má model. Teraz si môžeme všimnúť, že model T_c bude rôzny od štandardného modelu a nebude s ním ani izomorfný. Vieme teda, že neštandardný model existuje, ale nevieme ho skonštruovať.

Kapitola 3

Dokazovanie formúl – Metóda rezolvent

3.1 Metóda rezolvent

Celú túto kapitolu sa budeme venovať sémantike formúl logiky prvého rádu.

Keď uvažujeme výrokovú logiku, interpretujeme formulu A funkciou $\bar{v}$ – valuáciou. Formulu sme nazvali tautológiou, ak $\bar{v}(A)$ je pre každú interpretáciu pravda – treba preskúmať 2^n interpretácii. V predikátovej logike je to (ako uvidíme) ešte horšie.

Zopakujme si, čo už vieme. V predikátovej logike máme funkčné a predikátové symboly. Univerzum budem označovať netradične ako D. Znakom M budeme totiž označovať jadro(maticu) formuly v prenexnom tvare.

Funkcia f je realizovaná ako n-árna funkcia $f(x_1, \ldots, x_n) : D^n \to D$. Predikát P je realizovaný ako n-árna funckia $P(x_1, \ldots, x_n) : D^n \to \{0, 1\}$.

Vo formule rozlišujeme voľné a viazané premenné. Ak má formula voľné premenné, nevieme určiť jej pravdivostnú hodnotu, iba ak za všetky voľné premenné dosadíme konštanty.

Ďalej, ku každej formule A vieme zostrojiť takú, ktorá je v prefixovom (prenexnom) tvare – t.j. je tvaru prefix + jadro: $(Q_1x_1)\cdots(Q_nx_n)M$.

Na upravenie formuly do tohoto tvaru používame prenexné operácie. Skutočnosť, že premenná x má voľný výskyt vo formule A budeme značiť ako $A(x)$, v opačnom prípade budeme písať jednoducho A.

Prenexné operácie:

$$(Qx)A(x) \vee B \equiv (Qx)(A(x) \vee B) \tag{1a}$$
$$(Qx)A(x) \wedge B \equiv (Qx)(A(x) \wedge B) \tag{1b}$$
$$\neg(\forall x)A(x) \equiv (\exists x)\neg A(x) \tag{2a}$$
$$\neg(\exists x)A(x) \equiv (\forall x)\neg A(x) \tag{2b}$$
$$(\forall x)A(x) \wedge (\forall x)B(x) \equiv (\forall x)(A(x) \wedge B(x)) \tag{3a}$$
$$(\exists x)A(x) \vee (\exists x)B(x) \equiv (\exists x)(A(x) \vee B(x)) \tag{3b}$$

Poznámka 3.1.1 *(:* S predchádzajúcimi operáciami 3a,3b treba pracovať pozorne. Im veľmi podobné úpravy totiž neplatia:

$$(\forall x)A(x) \vee (\forall x)B(x) \not\equiv (\forall x)(A(x) \vee B(x)) \tag{x1}$$
$$(\exists x)A(x) \wedge (\exists x)B(x) \not\equiv (\exists x)(A(x) \wedge B(x)) \tag{x2}$$

Zoberme si napríklad $D = \{1, 2\}$. Ak položíme $A(1) = 1, A(2) = 0, B(1) = 0, B(1) = 1$, dostaneme, že pravá strana x1 bude platiť, zatiaľ čo ľavá strana nie. Pre x2 naopak. *:)*

Pretože môžeme substituovať za premenné – $(\forall x)B(x) \equiv (\forall z)B(z)$, môžeme predchádzajúce prenexné operácie zhrnúť do nasledujúcich všeobecných transformácií.

$$(Q_1x)A(x) \vee (Q_2x)B(x) \equiv (Q_1x)(Q_2z)(A(x) \vee B(z)) \tag{4a}$$
$$(Q_3x)A(x) \wedge (Q_4x)B(x) \equiv (Q_3x)(Q_4z)(A(x) \wedge B(z)) \tag{4b}$$

kde v oboch prípadoch z je premenná, ktorá sa nevyskytuje voľne v A (a ani v pôvodnom $B(x)$). Tento najvšeobecnejší tvar ale zbytočne pridáva premenné a preto je vhodný iba v prípadoch, keď nefungujú operácie 1 až 3.

3.1.1 Algoritmus na zostrojenie prenexného tvaru

1. Odstránenie implikácií a ekvivalencií:

$$A \leftrightarrow B \equiv (A \rightarrow B) \wedge (B \rightarrow A)$$
$$A \rightarrow B \equiv \neg A \vee B$$

2. Odstránenie dvojitej negácie a presun negácie k formule.

$$\neg(\neg A) \equiv A$$
$$\neg(A \vee B) \equiv (\neg A \wedge \neg B)$$
$$\neg(A \wedge B) \equiv (\neg A \vee \neg B)$$
$$\neg(\forall x)A(x) \equiv (\exists x)\neg A(x)$$
$$\neg(\exists x)A(x) \equiv (\forall x)\neg A(x)$$

3. Premenovanie viazaných premenných, ak je to potrebné.

4. Použijeme zákony:

$$(Qx)A(x) \vee B \equiv (Qx)(A(x) \vee B)$$
$$(Qx)A(x) \wedge B \equiv (Qx)(A(x) \wedge B)$$
$$(\forall x)A(x) \wedge (\forall x)B(x) \equiv (\forall x)(A(x) \wedge B(x))$$
$$(\exists x)A(x) \vee (\exists x)B(x) \equiv (\exists x)(A(x) \vee B(x))$$
$$(Q_1x)A(x) \vee (Q_2x)B(x) \equiv (Q_1x)(Q_2z)(A(x) \vee B(z)) \text{ kde } z \text{ je nová premenná}$$
$$(Q_3x)A(x) \wedge (Q_4x)(B(X) \equiv (Q_3x)(Q_4z)(A(x) \wedge (B(z)) \text{ kde } z \text{ je nová premenná}$$

Príklad 3.1.1

$$(\forall x)(\forall y)\left[(\exists z)\left(P(x,z) \wedge P(y,z)\right) \rightarrow (\exists u)Q(x,y,u)\right] \equiv$$
$$(\forall x)(\forall y)\left[\neg(\exists z)(P(x,z) \wedge P(y,z)) \vee (\exists u)Q(x,y,u)\right] \equiv$$
$$(\forall x)(\forall y)\left[(\forall z)(\neg P(x,z) \vee \neg P(y,z)) \vee (\exists u)Q(x,y,u)\right] \equiv$$
$$(\forall x)(\forall y)(\forall z)(\exists u)\left[\neg P(x,z) \vee \neg P(y,z) \vee Q(x,y,u)\right]$$

3.2 Herbrandova veta - história

[FIXME: **Nasledujúca časť potrebuje skontrolovať a upraviť**]

Leibniz (1646 – 1716), Peáno (1900), Hilbertova škola (1920), Herbrand (1930). Fundamentálny výsledok, ktorý dal odpoveď na otázku, či existuje všeobecná procedúra, ktorá vie zistiť, či je daná formula tautológia, dali Church a Turing (1936, nezávisle od seba) – ukázali, že v predikátovej logike nie je problém rozhodnuteľnosti riešiteľný.

Herbrandova metóda je založená na procedúre vyvrátenia. Ide o nájdenie interpretácie, pri ktorej daná formula nie je splnená. Ak formula nie je tautológia, v konečnom počte krokov sa procedúra zastaví, pokiaľ ale nie je, procedúra pokračuje vo výpočte.

Gilmore (1960), Davis a Putnem (1960) – navrhovali procedúry, ktoré by boli schopné overovať tautologickosť formúl; fungovali ale iba pre jednoduchšie formuly.

V rokoch 1965 – 1968 Robinson zaviedol pojem resolventa (v podstate iným spôsobom zapísane pravidlo modus ponens. ———————————
Koniec neoverenej časti

3.3 Skolemovské štandardné formuly

Budeme sa zaoberať procedúram založených na Herbrandovej myšlienke vyvrátenia (nájdenie interpretácie, ktorá vyvracia danú formulu). Davis a Putnam pracovali s formulou v prefixovom normálnom tvare a vychádzali z nasledujúcich hľadísk:

1. Každá formula logiky 1. rádu môže byť vyjadrená v prefixovom normálnom tvare.
2. Pretože matica (jadro) neobsahuje kvantifikátory, môže byť vyjadrená v konjunktívnej normálnej forme.
3. Zachovajúc nesplniteľnosť formoly z nej môžeme eliminovať existenčné kvantifikátory pomocou tzv. skolemovských funkcií (keď máme premennú vyjadrenú v prefixovom normálnom tvare a eliminujeme z nej existenčný kvantifikátor, dostaneme formulu, ktorá je nesplniteľná vtedy, keď je nesplniteľná pôvodná formula – nesplniteľnosť transformovanej formuly sa robí ľahšie).

Transformácia formuly: Majme formulu $A : (Q_1x_1)(Q_2x_2)\dots(Q_nx_n)M$, kde M je konjunktívnom normálnom tvare. Nech Q_r je existenčný kvantifikátor v prefixe $(Q_1x_1)\dots(Q_nx_n)$, $1 \leq r \leq n$.

Uvažujme, že vľavo od Q_r nestojí žiaden veľký kvantifikátor. Vtedy, ak z prefixu vynechám (Q_rx_r) a x_r v M nahradím novou konštantou c_r a mám formulu, ktorá je nesplniteľná práve vtedy, keď bola nesplniteľná pôvodná formula.

Na druhej strane, naľavo od Q_r sa môžu vyskytovať všeobecné kvantifikátory, $Q_{s_1}, Q_{s_2}, \dots Q_{S_m}$, kde $1 \leq s_1 < s_2 < \dots < s_m < r$. Vtedy opäť odstránime (Q_rx_r) z prefixu a za premennú x_r dosadíme do M term $f(x_{s_1}, \dots, x_{s_m})$. Takúto funkciu voláme skolemovaská funkcia a podobne, takúto konštantu c voláme skolemovská konštanta.

Tento postup môžeme zopakovať pre všetky existenčné kvantifikátory a výsledok nazveme štandardnou skolemovskou formou.

Príklad 3.3.1 Nájdite štandardnú formu pre formuly:

$$(\exists x)(\forall y)(\forall z)(\exists u)(\forall v)(\exists w)P(x, y, z, u, v, w)$$

Premennú x budeme nahrádzať konštantou c (ktorá nie je v predikáte), premennú u nahradíme $f(y, z)$ a premennú w nahradíme funkciou $g(y, z, v)$. Výsledkom je

$$(\forall y)(\forall z)(\forall w)P(c, y, z, f(y, z), v, g(y, z, v))$$

Príklad 3.3.2 Nájdite štandardnú formu pre formulu:

$$(\forall x)(\exists y)(\exists z)\left[(\neg P(x, y) \wedge Q(x, z)) \vee R(x, y, z)\right]$$

Využijeme distributívne zákony pre logické spojky a dostaneme

$$(\forall x)(\exists y)(\exists z)\left[\Big(\neg P(x,y)\vee R(x,y,z)\Big)\wedge\Big(Q(x,z)\vee R(x,y,z)\Big)\right]$$

a po Skolemizácii máme

$$(\forall x)\left[\Big(\neg P(x,f(x))\vee R(x,f(x),g(x))\Big)\wedge\Big(Q(x,g(x))\vee R(x,f(x),g(x)\Big)\right]$$

Poznámka 3.3.1 *(:* Formula môže mať viacero štandardných foriem. *:)*

Definícia 3.3.1 (Literál) *Atóm (predikát), alebo jeho negácia.*

Definícia 3.3.2 (Klauzula) *Disjunkcia literálov. Špeciálne jednotková klauzula (tiež jednoliterálna klauzula) obsahuje jeden literál.*

Definícia 3.3.3 (Prázdna klauzula) *Klauzala neobsahujúca žiaden literál, (označujeme ju ε). Prázdna klauzula je nesplniteľná, pretože neobsahuje žiaden literál, ktorý by mohol byť splniteľný.*

Poznámka 3.3.2 *(:* Ak sa nad tým, zamyslíme, definovali sme si nesplniteľnosť prázdnej klauzuly tak, aby výraz $\varepsilon\vee K$ bol ekvivalentný výrazu K a aby nesplniteľnosť výrazu $\varepsilon\wedge K$ bola ekvivalentná nesplniteľnosti výrazu K. *:)*

Poznámka 3.3.3 *(:* Štandardná skolemovská forma sa dá zadať aj v množinovom zápise. Presnejšie povedané, štandardná forma je konjunkcia klauzulí a za jej množinu budeme považovať množinu týchto klauzúl. Takýto zápis budeme často využívať a ako uvidíme, tieto dva zápisy sú si plne ekvivalentné, čo sa týka nesplniteľnosti. *:)*

Príklad 3.3.3 Uvažujme formulu $P\wedge Q\wedge\neg R$.[1] Ako vieme ju zapísať ako množinu klauzúl v konjunkcii nasledovne $\{P,Q,\neg R\}$. Podobne, pre štandardnú formu

$$(\forall x)\left[\Big(\neg P(x,f(x))\vee R(x,f(x),g(x))\Big)\wedge\Big(Q(x,g(x))\vee R(x,f(x),g(x)\Big)\right]$$

z minulého príkladu vieme spraviť ekvivalentný množinový zápis ako

$$\{\neg P(x,f(x))\vee R(x,f(x),g(x)),\quad Q(x,g(x))\vee R(x,f(x),g(x)\}$$

Veta 3.3.1 *Nech $\mathscr{S}$ je množina klauzúl, ktoré tvoria štandardnú formu formuly A. Potom A nie je splniteľná $\iff$ $\mathscr{S}$ nie je splniteľná.*

Dôkaz: Uvažujme formulu A tvaru $A:(Q_1x_1)\dots(Q_nx_n)M[x_1,\dots x_n]$. Nech Q_r je prvý existenčný kvantifikátor, čiže A je tvaru $(\forall x_1)(\forall x_2)\dots(\forall x_{r-1})(\exists x_r)(Q_{r+1}x_{r+1})\dots(Q_nx_n)M[x_1,\dots x_n]$. Existenčný kvantifikátor nahradíme novou $(r-1)$-árnou funkciou f a dostávame formulu A_1 v tvare

$$A_1:(\forall x_1)\dots(\forall x_{r-1})(Q_{r+1}x_{r+1})\dots(Q_nx_n)M[x_1,\dots,x_{r-1},f(x_1,\dots,x_{r-1}),x_{r+1},x_n]$$

Tvrdíme, že A nie je splniteľná práve vtedy keď A_1 nie je splniteľná:

- $\Rightarrow$: Sporom. Nech A_1 je splniteľná. Potom existuje taká interpretácia I, že I vyhovuje A_1 (A_1 je pravdivé v I). To znamená, že pre všetky $x_1,\dots,x_{r-1}$ existuje také x_r, ktoré je rovné $f(x_1,\dots,x_{r-1})$. Tá istá interpretácia teda vyhovuje aj pôvodnej formule A.
- $\Leftarrow$: Opäť sporom. Nech A je splniteľná. Teda existuje interpretácia I, ktorá vyhovuje formule A. Potom pre každú $r-1$-ticu $x_1,\dots,x_{r-1}$ existuje také x_r, že platí $M[x_1,\dots,x_{r-1},x_r,\dots,x_n]$. Rozšírme I o $(r-1)$-árny funkčný symbol f tak, že $f(x_1,\dots,x_{r-1})=x_r$. Potom I' vyhovyje formule A_1 a teda dostávame spor.

[1] Toman na tomto mieste píše $P\vee Q\vee\neg R$, som si však takmer istý, že to pôvodne myslel opačne.

Pokračujme ďalej v dôkaze: Označme pôvodnú formulu ako A_0. Potom môžeme dosiahnuť štandardnú formu S ako postupnosť $A_0, A_1, \ldots, A_m$, kde každý krok je zámena prvého existenčného kvantifikátora vo formule A_i. Ak A_i nie je splniteľná, tak ani A_{i+1} nie je splniteľná. Tým pádom A_0 nie je splniteľná $\iff$ A_1 nie je splniteľná $\iff$ $\ldots$ $\iff$ $A_m \equiv S$ nie je splniteľná. No a S nie je splniteľná práve vtedy keď $\mathscr{S}$ nie je splniteľná.[2]
■

Poznámka 3.3.4 *(: Ak A nie je splniteľná, tak nesplniteľnosť A je ekvivalentná nesplniteľnosti množinovej verzie štandardnej formy $\mathscr{S}$, teda môžeme písať $A \equiv \mathscr{S}$. :)*

Poznámka 3.3.5 *(: Ak A je splniteľná, tak tvrdenie neplatí. Majme formulu A, ktorá je $A : (\exists x)P(x)$. Tým pádom štandardná forma S je $S : P(a)$ (x sme nahradili skolemovskou konštantou a). Vezmime interpretáciu s univerzom $D = \{1, 2\}$, pričom a priradíme v I hodnotu 1. Hodnoty pre P budú $P(1) = false, P(2) = true$. Potom ale A je splniteľná v I (existuje také x, menovite 2), lenže $P(a)$ nie je splniteľná v interpretácii I. Preto $A \not\equiv S$. :)*

Poznámka 3.3.6 *(: Z predchádzajúcej poznámky sa ukazuje, že metódy dokazovania formúl budú založené na vyvrátení negácie. :)*

Poznámka 3.3.7 *(: Majme formulu $A : A_1 \wedge A_2 \wedge \ldots \wedge A_n$. Pre každé A_i si vytvoríme štandardnú formulu S_i. Potom štandardná forma pre A je $\mathscr{S} = \mathscr{S} \cup \mathscr{S} \cup \ldots \cup \mathscr{S}$, kde $\mathscr{S}$ je množina klauzúl štandardnej formu S_i. Formula A nie je splniteľná práve vtedy, keď nie je splniteľná množina klauzúl $\mathscr{S}$. :)*

Príklad 3.3.4 (Z teórie grúp) Uvedieme príklad, kde sa pokúsime zapísať pomocou množiny klauzúl tvrdenie z teórie grúp.

Uvažujme grupu a na nej operáciu $\circ$. Platia nasledovné axiomy:

$A_1 : x, y \in G \Rightarrow x \circ y \in G$ – vlastnosť uzavretosti.

$A_2 : x, y, z \in G \Rightarrow (x \circ y) \circ z = x \circ (y \circ z)$ – asociatívnosť operácie.

$A_3 : x \in G \Rightarrow x \circ e = e \circ x = x$ – existencia neutrálneho prvku.

$A_4 : x \in G \Rightarrow \exists x^{-1} \in G : x \circ x^{-1} = e = x^{-1} \circ x$ – existencia inverzného prvku.

Chceme ukázať, že ak pre všetky $x \in G$ platí $x \circ x = e$, potom je grupa komutatívna. Prvou časťou úlohy je formalizovanie zadania: Nech $P(x, y, z)$ označuje[3] $x \circ y = z$ a nech $i(x) = x^{-1}$.

Prepísané axiómy vyzerajú nasledovne:

$$
\begin{aligned}
A_1' &: (\forall x)(\forall y)(\exists z)P(x, y, z) \\
A_2' &: \begin{array}{l} (\forall x)(\forall y)(\forall z)(\forall u)(\forall v)(\forall w)[(P(x, y, u) \wedge P(y, z, v) \wedge P(u, z, w)) \rightarrow P(x, v, w)] \\ \wedge\ (\forall x)(\forall y)(\forall z)(\forall u)(\forall v)(\forall w)[(P(x, y, u) \wedge P(y, z, v) \wedge P(x, v, w)) \rightarrow P(u, z, w)] \end{array} \\
A_3' &: (\forall x)P(x, e, x) \wedge (\forall x)P(e, x, x) \\
A_4' &: (\forall x)P(x, i(x), e) \wedge (\forall x)P(i(x), x, e)
\end{aligned}
$$

Späť k nášmu tvrdeniu. Chceme ukázať

$$
\begin{aligned}
(\forall x \in G : x \circ x = e) &\Rightarrow (\forall u, v \in G : u \circ v = v \circ u) \\
B' &: (\forall x)P(x, x, e) \rightarrow (\forall u)(\forall v)[P(u, v, w) \rightarrow P(v, u, w)]
\end{aligned}
$$

[2] Viď poznámku 3.3.7.

[3] Na tomto mieste by som poznamenal, že to má Toman spravené výrazne pofidérne. Totiž, nahradením funkcie predikátom sme stratili jednoznačnosť funkčnej hodnoty, teda, momentálne môže platiť $P(x, y, z) \wedge P(x, y, z') \wedge z \neq z'$. Jednoduchou interpretáciou, ktorá spĺňa všetky axiómy je napríklad $P \equiv true$ a evidentne takáto realizácia nie je teóriou grúp.

Na druhej strane, spomínaná Tomanova teória je korektná. Pointa tkvie v tom, že Tomanova teória *nemá* predikát rovnosti (čo ruší naše argumenty). Mohlo by sa zdať, že daná teória je potom akosi okliešťená, čo aj je. Predikát rovnosti "$a = b$" sa ale formálne dá nahradiť predikátom "$P(a, e, b)$". Takto definovaná "rovnosť" vyhovuje všetkým axiómam rovnosti a navyše sa v nej nedá použiť protipríklad uvedený vyššie. Teória je teda v poriadku.

Teraz potrebujeme ukázať, že $A'_1 \wedge A'_2 \wedge A'_3 \wedge A'_4 \to B'$. Vytvoríme negáciu výroku a ukážeme, že nie je splniteľná:

$$F' : \neg(A'_1 \wedge A'_2 \wedge A'_3 \wedge A'_4) \vee B'$$
$$\neg F' : A'_1 \wedge A'_2 \wedge A'_3 \wedge A'_4 \wedge \neg B'$$

Ideme vytvárať množinu klauzúl. Prevedením A'_1, A'_2, A'_3, A'_4 do štandardnej formy dostávame

$$\mathscr{S}_1 : \Big\{P(x, y, f(x, y))\Big\}$$
$$\mathscr{S}_2 : \begin{Bmatrix}\neg P(x, y, u) \vee \neg P(y, z, v) \vee \neg P(u, z, w) \vee P(x, v, w), \\ \neg P(x, y, u) \vee \neg P(y, z, v) \vee \neg P(x, v, q) \vee P(u, z, w)\end{Bmatrix}$$
$$\mathscr{S}_3 : \Big\{P(x, e, x),\ P(e, x, x)\Big\}$$
$$\mathscr{S}_4 : \Big\{P(x, i(x), e),\ P(i(x), x, e)\Big\}$$

Ostáva nám vyjadriť $\neg B'$ ako množinu $\mathscr{B}$.

$$\begin{aligned}\neg B' : \neg[(\forall x)P(x, x, e) \to (\forall u)(\forall v)(\forall w)(P(u, v, w) \to P(v, u, w))] &\iff \\ \neg[\neg(\forall x)(P(x, x, e) \vee (\forall u)(\forall v)(\forall w)(\neg P(u, v, w) \vee P(v, u, w))] &\iff \\ (\forall x)(P(x, x, e) \wedge \neg(\forall u)(\forall v)(\forall w)[\neg P(u, v, w) \vee (P(v, u, w)] &\iff \\ (\forall x)P(x, x, e) \wedge (\exists u)(\exists v)(\exists w)[P(u, v, w) \wedge \neg P(v, u, w)]\end{aligned}$$

Množina $\mathscr{B}$ je potom

$$\mathscr{B} : \Big\{P(x, x, e),\ P(a, b, c),\ \neg P(b, a, c)\Big\}$$

Máme dokázať, že množina klauzúl $\mathscr{S} = \mathscr{S}_1 \cup \mathscr{S}_2 \cup \mathscr{S}_3 \cup \mathscr{S}_4 \cup \mathscr{B}$ nie je splniteľná. Teda pre každú oblasť a interpretáciu je nesplniteľná. Bolo by teda potrebné vyšetriť všetky oblasti. Toto je ale príliš zložité – overiť niečo na všetkých možných oblastiach je nad naše sily. Nám ale bude stačiť vyšetrovať na *Herbrandovskom univerze*, ako si ukážeme v nasledujúcej stati.

3.4 Herbrandovské univerzum

Poznámka 3.4.1 *(:* V nasledujúcom texte budeme používať a medzi sebou zamieňať nasledujúce výrazy s rovnakým významom: "nie je splniteľná", "je sporná" a "je protirečivá". Taktiež, občas budeme zamieňať medzi sebou aj ich negácie. *:)*

Definícia 3.4.1 (Herbrandovské univerzum množiny klauzúl) *Nech H_0 je množina konštánt, ktoré sa vyskytujú v množine klauzúl S. Ak S neobsahuje žiadnu konštantu, tak položíme $H_0 = \{a\}$, kde a je nejaká konštanta. Ďalej definujme H_{i+1} ako zjednotenie H_i a množiny všetkých termov tvaru $f^{(n)}(t_1, \ldots, t_n)$, kde $f^{(n)} \in S$ a $t_1, \ldots, t_n \in H_i$. Množinu H_i nazývame* herbrandovské univerzum *i-tej úrovne. Herbrandovské univerzum množiny klauzúl definujeme ako zjednotenie cez všetky úrovne:*

$$H = \bigcup_{i=0}^{\infty} H_i$$

Príklad 3.4.1 Majme množinu klauzúl $S = \{P(a),\ \neg P(x) \vee \neg P(f(x))\}$. Potom herbrandovské

univerzá jednotlivých úrovní sú

$$\begin{aligned}
H_0 &= \{a\} \\
H_1 &= \{a,\ f(a)\} \\
H_2 &= \{a,\ f(a),\ f(f(a))\} \\
&\vdots \\
H &= \{a,\ f(a),\ f(f(a),\ f(f(f(a))),\ \dots\}
\end{aligned}$$

Príklad 3.4.2 Nech $S = \{P(x) \vee R(x),\ R(z),\ T(y) \vee \neg W(y)\}$, teda množina S neobsahuje žiadnu konštantu. Preto kladieme $H_0 = \{a\}$. Dostávame $H_0 = H_1 = \cdots = H = \{a\}$.

Príklad 3.4.3 Uvažujme množinu klauzúl $S = \{P(f(x), a, g(y), b)\}$. Potom

$$\begin{aligned}
H_0 =& \{a,\ b\} \\
H_1 =& \{a,\ b,\ f(a),\ g(a),\ f(b),\ g(b)\} \\
H_2 =& \{a,\ b,\ f(a),\ g(a),\ f(b),\ g(b),\ f(f(a)),\ f(f(b)), \\
& f(g(b)),\ f(g(b)),\ g(f(a)),\ g(f(b)),\ g(g(a)),\ g(g(b))\}
\end{aligned}$$

Definícia 3.4.2 (Výraz) *Pod pojmom výraz budeme chápať term, množinu termov, klauzulu, množinu klauzúl, atóm, množinu atómov, literál, množinu literálov.*

Definícia 3.4.3 (Podvýraz) *Podvýraz výrazu F je ľubovoľný výraz, ktorý sa vyskytuje v F.*

Definícia 3.4.4 (Základný výraz) *Ľubovoľný výraz, ktorý neobsahuje premenné, sa nazýva základný výraz (základný term, základný atóm, základná klauzula, základný literál, ...).*

Definícia 3.4.5 (Základná inštancia) *Základnou inštanciou klauzuly C z množiny klauzúl S je klauzula, ktorú dostaneme zámenou všetkých premenných za prvky Herbrandovského univerza.*

Príklad 3.4.4 Majme množinu $S = \{P(x),\ Q(f(x)) \vee R(y)\}$ a majme klauzulu $C : P(x)$. Herbrandovské univerzum H je $H = \{a,\ f(a),\ f(f(a)),\ f(f(f(a))),\ \dots\}$. Základné inštancie pre C sú $P(a), P(f(a)), P(f(f(a))), \dots$.

Definícia 3.4.6 (Herbrandovská báza) *Nech S je množina formúl. Potom množina atómov tvaru $P^{(n)}(t_1, \dots, t_n)$ pre všetky n-árne predikáty, ktoré sa vyskytujú v S a všetky termy t_i z Herbrandovského univerza nazývame Herbrandovskou bázou S. Sú to atómy takého tvaru, že sa v nich nevyskytuje žiadna premenná.*

Položme si otázku, čo znamená interpretovať množinu klauzúl S na Herbrandovskom univerze H. Musíme poznať hodnoty konštánt, interpretáciu funkčných a predikátových symbolov. Budeme uvažovať špeciálnu interpretáciu, takzvanú H-interpretáciu, pri ktorej nebudeme interpretovať predikátové symboly (necháme si to ako keby na neskôr).

Definícia 3.4.7 (H-interpretácia) *Nech S je množina klauzúl. Ďalej nech H je herbrandovské univerzum pre množinu klauzúl S a I je interpretácia v množine klauzúl S nad H. Hovoríme, že interpretácia I je herbrandovská interpretácia (alebo tiež H-interpretácia), ak platí:*

1. *Interpretácia I zobrazuje všetky konštanty na samé seba, t.j. konštante $a \in S$ priradí tú istú konštantu $a \in H$.*
2. *Nech $f^{(n)}$ je n-árny funkčný symbol a $h_1, \dots, h_n$ sú prvky herbrandovského univerza H. Potom funkciu f budeme v I realizovať ako funkciu, ktorá zobrazuje $(h_1, \dots, h_n) \in H^n$ na element $f^{(n)}(h_1, \dots, h_n) \in H$.*

Poznámka 3.4.2 *(:* Ako sme už spomínali, nekladieme žiadne obmedzenia na interpretáciu predikátov.

Uvažujme ako príklad množinu $A = \{A_1, A_2, \dots\}$. Nech je to herbrandovská báza pre množinu klauzúl S. Herbrandovskú interpretáciu určíme tak, že I zadáme ako $I = \{m_1, m_2, \dots\}$, kde m_i bude buď A_j (ak A_j je pravdivé) alebo $\neg A_j$ (ak A_j je nepravdivé). *:)*

Príklad 3.4.5 Majme množinu klauzúl $S = \{P(x) \vee Q(x),\ R(f(y))\}$. Herbrandovské univerzum je $H = \{a,\ f(a),\ f(f(a)),\ \dots\}$. V S sa vyskytujú unárne predikáty P, Q, R. Herbrandovská báza je potom

$$A : \{P(a),\ Q(a),\ R(a),\ P(f(a)),\ Q(f(a)),\ R(f(a)),\ \dots\}.^4$$

Môžeme mať nasledovné interpretácie:

$$I_1 : \{P(a),\ Q(a),\ R(a),\ P(f(a)),\ Q(f(a)),\ R(f(a)),\ \dots\}$$

teda, predikáty sú vždy pravdivé. Alebo

$$I_2 : \{\neg P(a),\ \neg Q(a),\ \neg R(a),\ \neg P(f(a)),\ \neg Q(f(a)),\ \neg R(f(a)),\ \dots\}$$

čiže predikáty nie sú nikdy pravdivé. Ďalšia možná interpretácia je

$$I_3 : \{P(a),\ Q(a),\ \neg R(a),\ P(f(a)),\ Q(f(a)),\ \neg R(f(a)),\ \dots\}$$

V zásade pre každú možnú kombináciu si vieme vytvoriť interpretáciu.

Ďalšou úlohou bude k ľubovoľnej interpretácii nad ľubovoľným univerzom priradiť Herbrandovskú interpretáciu a zaviesť príslušné tvrdenia a definície.

Príklad 3.4.6 Majme množinu klauzúl $S = \{P(x),\ Q(y, f(y, a))\}$. Nech je oblasť interpretácie $D = \{1, 2\}$ a interpretujme konštanty, funkčné symboly a predikátové symboly podľa tabuľky 3.1

symbol	a	f(1,1)	f(1,2)	f(2,1)	f(2,2)
hodnota	2	1	2	2	1

predikát	P(1)	P(2)	Q(1,1)	Q(1,2)	Q(2,1)	Q(2,2)
hodnota	true	false	false	true	false	true

Tabuľka 3.1: Interpretácia I z príkladu 3.4.6

Ideme určiť H-interpretáciu I^*, ktorá akýmsi spôsobom bude prislúchať našej interpretácii I. Najskôr si určíme bázu:

$$A = \{P(a),\ Q(a,a),\ P(f(a,a)),\ Q(a, f(a,a)), Q(f(a,a), a),\ \dots\}$$

Hodnoty pre príslušné predikáty I^* určíme pomocou zadaných tabuliek pre I:

$$\begin{aligned}
P(a) = P(2) &= false \\
Q(a,a) = Q(2,2) &= true \\
P(f(a,a)) = P(f(2,2)) &= P(1) = true \\
Q(f(a,a), a) = Q(f(2,2), 2) &= Q(1,2) = true \\
Q(a, f(a,a)) = Q(1, f(2,2)) &= Q(2,1) = false \\
Q(f(a,a), f(a,a)) = Q(f(2,2), f(2,2)) &= Q(1,1) = false
\end{aligned}$$

Interpretácia I^* je teda

$$I^* = \{\neg P(a),\ Q(a,a),\ P(f(a,a)),\ \neg Q(a, f(a,a)),\ Q(f(a,a), a),\ \dots\}$$

[4] Všimnime si, že v danej množine je aj $R(a)$, hoci by sme možno očakávali, že to musí začínať $R(f(a))$

Príklad 3.4.7 Môže nastať aj iný prípad – majme množinu klauzúl S, ktorá neobsahuje konštantu: $S = \{P(x),\ Q(y, f(y, z))\}$. Máme danú interpretáciu I s oblasťou $D = \{1, 2\}$ popísanú tabuľkou 3.2

symbol	f(1,1)	f(1,2)	f(2,1)	f(2,2)
hodnota	1	2	2	1

predikát	P(1)	P(2)	Q(1,1)	Q(1,2)	Q(2,1)	Q(2,2)
hodnota	true	false	false	true	false	false

Tabuľka 3.2: Interpretácia I z príkladu 3.4.7

Tejto interpretácii budú zodpovedať dve H-interpretácie I_1^* a I_2^*, pričom v prvej bude a interpretované ako 1 a v druhej ako 2.

$$I_1^* = \{\ P(a),\ \neg Q(a,a),\ P(f(a,a)),\ \neg Q(a,f(a,a)),\ \neg Q(f(a,a),a),\ \dots\}$$
$$I_2^* = \{\neg P(a),\ \neg Q(a,a),\ P(f(a,a)),\ \neg Q(a,f(a,a)),\quad Q(f(a,a),a),\ \dots\}$$

Teraz si formálne zavedieme, čo to znamená priradiť nejakej interpretácii I zodpovedajúcu H-interpretáciu I^*:

Definícia 3.4.8 (Zodpovedajúca H-interpretácia) *Majme interpretáciu I pre množinu klauzúl S na oblasti interpretácií D. Interpretácii I priradíme zodpovedajúcu H-interpretáciu I^* nasledovne: Nech $h_1, h_2, \dots, h_n$ sú prvky Herbrandovského univerza H. Nech každé h_i sa zobrazí v interpretácii I na prvok $d_i \in D$. Zoberme predikát $P^{(n)}$ z množiny klauzúl S. Definujeme splniteľnosť (a pravdivosť) predikátu P v I^* nasledovne: $P^{(n)}(h_1, \dots, h_n)$ je pravdivý v I^* práve vtedy keď je $P^{(n)}(d_1, \dots, d_n)$ pravdivý v I.*

Lema 3.4.1 *Majme interpretáciu I na oblasti D. Nech táto interpretácia vyhovuje množine klauzúl S. Potom ľubovoľná H-interpretácia I^*, ktorá je priradená (zodpovedá) I, taktiež vyhovuje množine klauzúl S.*

Dôkaz: Majme množinu klauzúl $S = \{C^{(1)}, C^{(2)}, \dots, C^{(n)}\}$. Nech klauzula $C^{(i)}$ je nasledujúca disjunkcia literálov $C^{(i)} = L_1^{(i)} \vee L_2^{(i)} \vee \dots \vee L_{r_i}^{(i)}$ pre $i = 1, \dots, n$. Ľubovoľný literál $L_j^{(i)}$ je buď atomická formula alebo jej negácia. Predpokladajme že interpretácia I na univeze D vyhovuje množine klauzúl S. Potom musí byť pravdivý aspoň jeden literál v každej klauzule $C^{(i)}$. Lenže pre tieto literály $L_j^{(i)}$ platí $L_j^{(i)} = P^{(n)}(d_1, \dots, d_n)$ je pravdivé v I a z toho dostávame $P^{(n)}(h_1, \dots, h_n)$ je pravdivé v I^*. Teda, ak I vyhovuje množine klauzúl S, bude jej vyhovovať aj I^*.
■

Veta 3.4.1 *Množina klauzúl S nie je splniteľná práve vtedy, keď S je nepravdivá pri všetkých H-interpretáciach S.*

Dôkaz:

$\Rightarrow$: Nech množina klauzúl S nie je splniteľná. Potom je nepravdivá pre ľubovoľnú interpretáciu na ľubovoľnej oblasti. Teda aj pre ľubovoľnú H-interpretáciu na H-univerze.

$\Leftarrow$: Nech množina klauzúl S je nepravdivá pre ľubovoľnú H-interpretáciu množiny klauzúl S. Pre spor predpokladajme, že existuje interpretácia I s oblasťou D pre množinu klauzúl S, ktorá vyhovuje S. Uvažujme I^*, ktorá je priradená (zodpovedá) interpretácii I pre množinu klauzúl S. Podľa lemy 3.4.1 ale vieme, že ak vyhovuje I, vyhovuje aj I^*, čo je spor.

■

Podarilo sa nám teda objaviť také univerzum (H-univerzum), pre ktoré stačí vyšetriť splniteľnosť množiny klauzúl S na všetkých interpretáciach a budeme vedieť povedať (ne)splniteľnosť formuly na ľubovoľnej interpretácii v ľubovoľnom univerze. Posunuli sme sa o krok bližšie k rozhodovaniu platnosti S.

Poznámka 3.4.3 *(:* V nasledujúcom texte budeme používať iba H-interpretácie. Preto sa dohodneme (na skrátenie a zjednodušenie zápisu), že ich budeme nazývať iba interpretácie a označovať ako I. *:)*

Poznámka 3.4.4 *(:* Zhrňme si niekoľko základných pozorovaní:

1. Majme klauzulu (disjunkciu literálov) C a nech C' je jej základná inštancia, t.j. každá premenná bola nahradená prvkom H-univerza. C' je splniteľná v (H-)interpretácii I práve vtedy, keď existuje základný literál $L' \in I$, ktorý je splniteľný. Teda C' je splniteľná $\iff C' \cap I \neq 0$.
2. Klauzula C je splnená v interpretácii $I \iff$ každá jej základná inštancia C' je splnená v I.
3. Klauzula C je odmietnutá (vyvrátená) v $I \iff$ existuje aspoň jedna taká základná inštancia C', ktorá nie je splniteľná (teda je vyvrátená) v I.
4. Množina klauzúl S nie je splniteľná $\iff$ pre každú interpretáciu I existuje aspoň jedna klauzula $C \in S$ a jej základná inštancia C', ktorá nie je splniteľná v I.

:)

Príklad 3.4.8 Uvažujme klauzulu $C = \neg P(x) \vee Q(f(x))$ a interpretácie I_1, I_2, I_3 definované nasledovne:

$$
\begin{aligned}
I_1 &= \{\neg P(a),\ \neg Q(a),\ \neg P(f(a)),\ \neg Q(f(a)),\ \neg P(f(f(a))),\ \neg Q(f(f(a))),\ \dots\} \\
I_2 &= \{\ \ P(a),\ \ \ Q(a),\ \ \ P(f(a)),\ \ \ Q(f(a)),\ \ \ P(f(f(a))),\ \ \ Q(f(f(a))),\ \dots\} \\
I_3 &= \{\ \ P(a),\ \neg Q(a),\ \ \ P(f(a)),\ \neg Q(f(a)),\ \ \ P(f(f(a))),\ \neg Q(f(f(a))),\ \dots\}
\end{aligned}
$$

Všímajme si klauzulu C a jednotlivé interpretácie: I_1 vyhovuje C (inak povedané C je splnená) a zabezpečujú to $\neg P(a),\ \neg P(f(a)),\ \neg P(f(f(a))), \dots$ Podobne, C je splnená v I_2 a zabezpečujú to $Q(a),\ Q(f(a)),\ Q(f(f(a))), \dots$ Naopak, C nie je splniteľná v I_3.

Príklad 3.4.9 Uvažujme množinu klauzúl $S = \{P(x),\ \neg P(x)\}$ a interpretácie $I_1 = \{P(a)\}, I_2 = \{\neg P(a)\}$.

Množina S nie je splnená ani jednou interpretáciou.

3.5 Sémantické stromy

Už sme povedali, že Herbrandovské interpretácie sú to pravé orechové, čo chceme overovať. Ostáva nám ale vyriešiť problém, ako ich nejakým spôsobom postupne preberať. A práve na to nám budú slúžiť sémantické stromy.

Definícia 3.5.1 (Kontrárna dvojica) *Majme nejaký literál (elementárna formulu) A. Dvojicu $\langle A, \neg A\rangle$ budeme nazývať kontrárnou dvojicou.*

Ak klauzula obsahuje kontrárnu dvojicu, potom je vždy platná a teda je to tautológia.

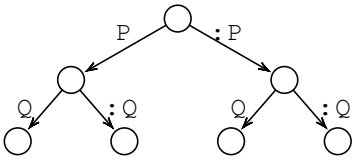
Definícia 3.5.2 (Sémantický strom) *Nech S je množina klauzúl a A je Herbrandovská báza pre množinu S. Pod sémantickým stromom pre množinu klauzúl S budeme rozumieť zakorenený dolu rastúci strom v ktorom je každej hrane pripísaná množina atómov alebo negácií atómov (teda vlastne množina literálov) z Herbrandovskej bázy, pričom platí:*

1. *Z každého vrchola stromu vychádza konečný počet hrán. Ooznačme ich ich $l_1, l_2, \ldots, l_n$. Nech Q_i je konjunkcia všetkých literálov pripísaných hrane l_i, potom požadujeme aby $Q_1 \vee Q_2 \vee \cdots \vee Q_n$ bola tautológia.*

2. *Označme pre vrchov v symbolom $I(v)$ zjednotenie všetkých množín literálov pripísaných hranám cesty, ktorá vedie z koreňa do vrcholu v. Potom $I(v)$ nesmie obsahovať kontrárne dvojice.*

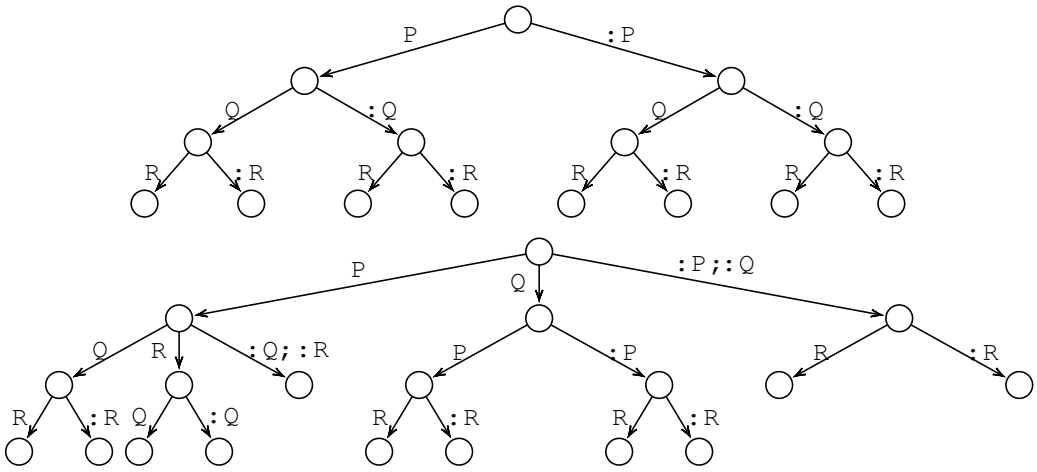
Definícia 3.5.3 (Úplný sémantický strom) *Nech $A = \{A_1, A_2, \ldots A_n\}$ je Herbrandovská báza pre množinu klauzúl S. Hovoríme, že sémantický strom prislúchajúci S je úplný, ak pre každý koncový vrchol(list) v platí: $I(v)$ obsahuje A_i alebo*[5] *$\neg A_i$ pre každé i.*

Príklad 3.5.1 Uvažujme množinu klauzúl $S = \{P, Q\}$. Potom úplný sémantický strom pre túto množinu môže vyzerať napríklad ako na obrázku 3.1.



Obr. 3.1: Jeden z možných sémantických stromov pre príklad 3.5.1

Príklad 3.5.2 K tej istej množine klauzúl môžeme mať viacero sémantických stromov, dokonca aj viacero úplných sémantických stromov. Uvažujme napríklad množinu klauzúl S, ktorá H-bázu $A : \{P, Q, R\}$. Potom 2 úplné sémantické stromy pre túto množinu sú naznačené na obrázku 3.2.

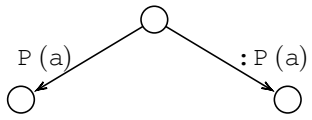


Obr. 3.2: Sémantické stromy pre príklad 3.5.2

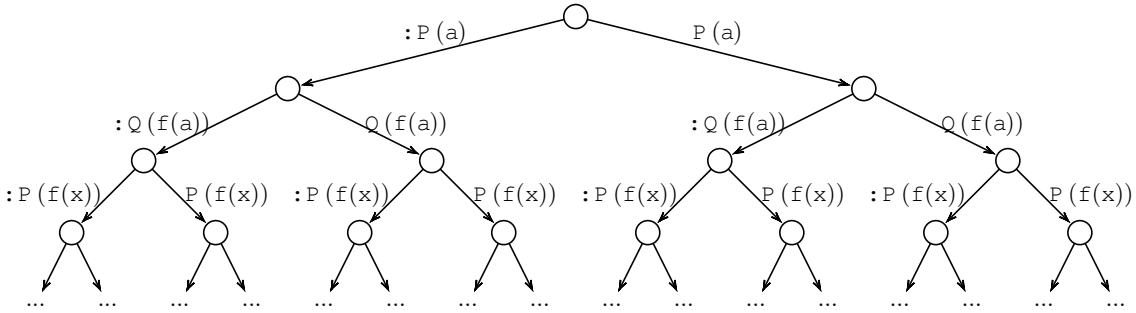
Príklad 3.5.3 Veľmi malý strom môžeme dostať v prípade, ak $S = \{P(x),\ P(a)\}$. Vtedy je báza $A : \{P(a)\}$ (nemáme žiadne funkčné symboly a teda si vystačíme s konštantou) a strom vyzerá nasledovne (obr. 3.3):

Príklad 3.5.4 Sémantický strom zďaleka nemusí byť konečný. Uvažujme napríklad množinu klauzúl $S = \{P(x), Q(f(x))\}$. Vtedy je herbrandovská báza nekonečná: $\{P(a),\ Q(a),\ P(f(a)),\ Q(f(a)),\ \ldots\}$. A pretože báza je nekonečná, musí byť nekonečný aj strom, ak chceme aby bol úplný. Jeden taký strom je znázornený na obrázku 3.4):

[5] Toto je exkluzívne alebo. Nemôže totiž platiť, že by obsahovala obe formuly



Obr. 3.3: Jeden z možných sémantických stromov pre príklad 3.5.3



Obr. 3.4: Nekonečný sémantický strom pre príklad 3.5.4

Poznámka 3.5.1 *(:* Radi by sme upozornili na istú drobnosť – definícia úplného stromu má isté problémy v prípade nekonečných stromov, pretože v nich nemáme koncové vrcholy. Preto definíciu upravíme nasledovne: Strom je úplný ak pre každú (nekonečnú) cestu platí, že obsahuje A_i pre všetky i. *:)*

Poznámka 3.5.2 *(:*

- Na úplný sémantický strom sa teda môžeme pozerať ako na organizované preberanie všetkých možných interpretácii.
- Navyše, na množinu $I(v)$ pre vrchol v sa môžeme pozerať ako na čiastočnú interpretáciu (interpretuje len niektoré prvky bázy).
- Už vieme, že množina klauzúl S je nesplniteľná $\iff$ je nepravdivá pre všetky herbrandovské interpretácie. Otázka znie, ako sa to prejaví na sémantickom strome. Vieme, že každá klauzula je konečný objekt. Preto sa musí nájsť nejaká konečná čiastočná interpretácia zamietajúca túto klauzulu.

  V prípade, ak množina základných inštancií $I'(v)$ prvkov $I(v)$ je odmietnutá, na tomto mieste môžeme prehľadávanie stromu ukončiť, pretože žiadna interpretácia nevyhovuje. Hovoríme tiež, že na tomto mieste môžeme strom odrezať.

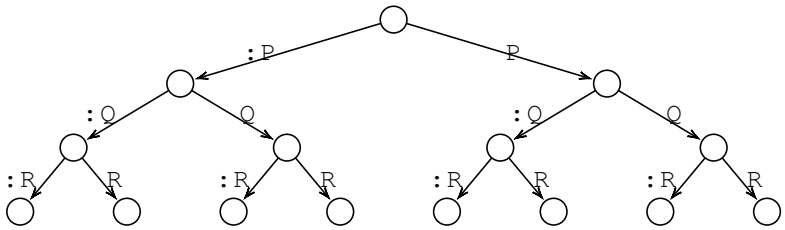
:)

Definícia 3.5.4 (Odmietajúci vrchol) *Vrchol v sémantického stromu pre množinu klauzúl S sa nazýva odmietajúcim, ak $I(v)$ odmieta niektorú základú inštanciu klauzuly z množiny S, no ľubovoľný vrchol v' na ceste z koreňa do vrcholu v neodmieta žiadnu základnú inštanciu klauzúl z S.*

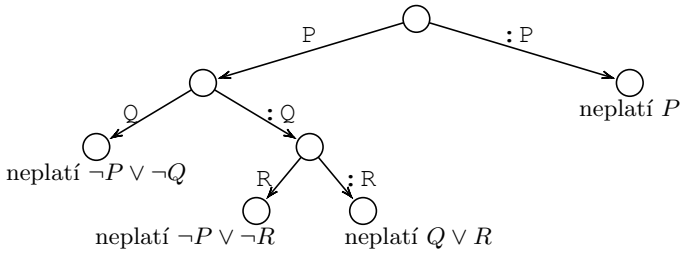
Definícia 3.5.5 (Uzavretý sémantický strom) *Hovoríme, že sémantický strom T pre množinu klauzúl S je uzavretý, ak každá vetva T končí odmietajúcim vrcholom.*

Definícia 3.5.6 (Akceptujúci vrchol) *Vrchol v sémantického stromu T pre množinu klauzúl S nazývame akceptujúcim, ak všetky nasledujúce vrcholy vrchola v sú odmietajúce.*

Príklad 3.5.5 Uvažujme množinu klauzúl $S = \{P,\ Q \vee R,\ \neg P \vee \neg Q,\ \neg R \vee \neg P\}$. Herbrandovskú báza je $\{P, Q, R\}$. Na obrázku 3.5.



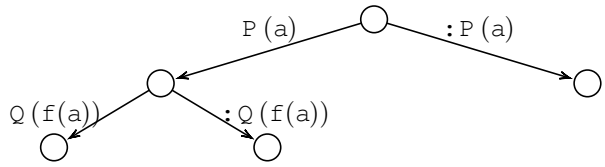
(a) Pôvodný strom



(b) Strom vzniknutý odrezaním odmietajúcich vrcholov

Obr. 3.5: Odrezanie sémantického stromu z príkladu 3.5.5

Príklad 3.5.6 Uvažujme množinu klauzúl $S = \{P(x),\ \neg P(x) \vee Q(f(x)),\ \neg Q(f(x))\}$.[6] Herbrandovská báza pre množinu klauzúl S je $\{P(a),\ Q(a),\ P(f(a)),\ Q(f(a)),\ \ldots\}$. Orezaný sémantický strom pre túto množinu klauzúl možno nájsť na obrázku 3.6.



Obr. 3.6: Odrezaný sémantický strom z príkladu 3.5.6

3.6 Herbrandova veta

Lema 3.6.1 (Dirichletov princíp) *Nech X, Y sú konečné množiny. Ak platí $|X| > |Y|$, potom pre každé zobrazenie $F : X \mapsto Y$ platí*

$$\exists y \in Y : \exists x_1, x_2 \in X :\ [x_1 \neq x_2] \wedge [f(x_1) = y = f(x_2)]$$

Tvrdenie možno rozšíriť aj na prípad, že X je nekonečná. Vtedy platí

$$\exists y \in Y : \textit{množina } \{x \in X : f(x) = y\} \textit{ je nekonečná}$$

Dôkaz: Dôkaz sa robí sporom. V prvom prípade dostaneme, že ak tvrdenie neplatí, f by mala byť injektívna, čo je ale spor s mohutnosťami. V druhom prípade X vieme rozložiť na niekoľko tried ekvivalencie podľa hodnoty $f(x)$ a nutne aspoň jedna z nich musí byť nekonečná.
■

Definícia 3.6.1 (Usporiadanie stromu) *Náš sémantický strom budeme chápať ako usporiadanú dvojicu $(T, \leq)$ kde T je množina vrcholov a "$\leq$" je relácia, ktorá čiastočne usporadúva T. Požadujeme, aby platilo*

[6] Na tomto mieste má Toman v poznámkach $P \vee Q(f(x))$ ale na prednáške to opravil

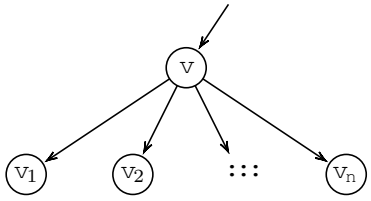
1. *$T(u) = \{v \in T, v < u\}$ je dobre usporiadaná (každá jej neprázdna podmnožina má najmenší prvok).*

2. *T má najmenší vrchol (koreň)*

Ak máme prvky u, v a neexistuje z také, že $u < z < v$, hovoríme, že prvok v nasleduje bezprostredne po prvku u.

Lema 3.6.2 (König) *Nech každý vrchol stromu s koreňom má konečné vetvenie (t.j. konečný stupeň vetvenia) a strom T je nekonečný. Potom v ňom existuje nekonečne dlhá vetva.*

Dôkaz: Uvažujme strom $(T_1, \leq)$ a vrchol $v \in T$. Označme množinu tých vrcholov, ktoré ležia pod v, teda $A_v = \{u \in T | v < u\}$. Nech $v_1, v_2, \ldots, v_n$ sú bezprostrední nasledovníci vrchola v (obr. 3.7). Potom platí



Obr. 3.7: Nasledovníci v

$$A_v = A_{v_1} \cup A_{v_2} \cup \ldots \cup A_{v_n} \cup \{v_1, v_2, \ldots, v_n\}$$

Predpokladáme, že A_v je nekonečná. Na základe Dirichletovho princípu potom jedna z množín A_{v_i} musí byť nekonečná.

Vybereme si x_0 ako koreň (najmenší vrchol stromu T). $A_{x_0} = T \backslash \{x_0\}$ a teda A_{x_0} je nekonečná. Teraz viem ale nájsť pre x_0 nasledovníka x_1, pre ktorý A_{x_1} je nekonečné. A pre ten vieme nájsť nasledovníka x_2, pre x_2 vieme nájsť x_3 atď. Vieme teda zostrojiť nekonečnú postupnosť nasledovníkov koreňa a teda v strome existuje nekonečne dlhá cesta z koreňa. ■

Po krátkej príprave sa môžeme pustiť do hlavnej časti, ktorá nás zaujíma. Budeme si formulovať Herbrandovu vetu, tradične v dvoch variantoch.

Veta 3.6.1 (Herbrandova, 1. variant) *Množina klauzúl S nie je splniteľná práve vtedy, keď ľubovoľnému úplnému sémantickému stromu pre množinu klauzúl S zodpovedá konečný uzavretý sémantický strom, t.j. ľubovoľná vetva úplného stromu vedie do odmietajúceho vrchola.*

Dôkaz:

$\Rightarrow$: Predpokladajme, že množina klauzúl S nie je splniteľná (nie je splniteľná pre ľubovoľnú H-interpretáciu). Nech T je úplný sémantický strom prislúchajúci množine S. Označme ako I_V množina všetkých literálov pripísaných vetve V stromu T. Potom I_V možno chápať ako interpretáciu množiny klauzúl S.

Predpokladajme, že S je nesplniteľná (teda nesplniteľná v každej interpretácii). To znamená, že pre klauzulu C existuje nejaká základná inštancia C', ktorá je v interpretácii I_V odmietnutá.

Ešte potrebujeme zabezpečiť, aby strom bol konečný. To ale musí byť, lebo ak by existovala nekonečná vetva, bola by to interpretácia, ktorá by neodmietala žiadnu zo základných inštancií.

$\Leftarrow$: Teraz predpokladáme, že k úplnému sémantickému stromu pre množinu klauzúl S existuje konečný uzavretý sémantický strom. Teda každá vetva stromu T končí v zamietajúcom vrchole. Nuž ale potom evidentne musí byť S odmietnutá v každej interpretácii a teda nie je splniteľná.

■

Veta 3.6.2 (Herbrandova, 2. variant) *Množina klauzúl S nie je splniteľná $\iff$ existuje konečná podmnožina S' základných inštancií klauzúl z S, ktorá nie je splniteľná.*

Dôkaz:

$\Rightarrow$: Predpokladajme, že množina klauzúl S nie je splniteľná. Na základe variantu 1 Herbrandovej vety platí, že ku každému úplnému sémantickému stromu T pre množinu klauzúl S existuje uzavretý konečný sémantický strom T'. Ak teraz zoberieme množinu základných inštancií klauzúl z T', ktoré prislúchajú odmietajúcim vrcholom (čiže listom), dostávame konečnú množinu $S' \subseteq S$, ktorá tiež nie je splniteľná.

$\Leftarrow$: Predpoklajme, že existuje konečná množina S' základných inštancií klauzúl S, ktorá nie je splniteľná. Vezmime si I interpretáciu S. Nech I' je "zúženie" interpretácie I na S'. Z nesplniteľnosťi S' vyplýva, že I' odmieta S'.

Interpretácia I obsahuje I', teda keď I' odmieta S', potom I odmieta S a teda S je nesplniteľná.

■

Príklad 3.6.1 Majme množinu klauzúl $S = \{P(x),\ \neg P(f(a))\}$. Chceme ukázať, že S nie je splniteľná. Na základe 2. Herbrandovej vety stačí nájsť konečnú podmnožinu množiny základných inštancií klauzúl, ktorá nie je splniteľná. Takáto množina je napríklad $S' = \{P(f(a)),\ \neg P(f(a))\}$.

Príklad 3.6.2 Majme množinu klauzúl $S = \{\neg P(x) \vee Q(f(x), x),\ P(g(b)),\ \neg Q(y, z)\}$. Táto množina nie je splniteľná – vezmime napríklad

$$S' = \{\neg P(g(b)) \vee Q(f(g(b)), g(b)),\ P(g(b)),\ \neg Q(f(g(b)), g(b))\}$$

Príklad 3.6.3 Uvažujme množinu klauzúl S:

$$\begin{aligned} S = \big\{ & \neg P(x, y, u) \vee \neg P(y, z, v) \vee \neg P(x, v, w) \vee P(u, z, w), \\ & \neg P(x, y, u) \vee \neg P(z, y, v) \vee \neg P(u, z, w) \vee P(x, v, w), \\ & P(g(x, y), x, y), \\ & P(x, h(x, y), y), \\ & P(x, y, f(x, y), \\ & \neg P(k(v), x, k(x)) \\ & \big\} \end{aligned}$$

Chceme ukázať, že S nie je splniteľná. Návod je napríklad takýto: Zostrojme si konečný uzavretý sémantický strom pre S a potom vypíšme základné inštancie klauzúl pripísaných jednotlivým cestám (vetvám) tohoto stromu. Možné riešenie je tak napríklad

$$\begin{aligned} S' = \big\{ & P(a, h(a, a), a), \\ & P(g(a, k(h(a, a))), a, k(h(a, a))), \\ & \neg P(k(h(a, a)), h(a, a), k(h(a, a))), \\ & \neg P(g(a, k(h(a, a))), a, k(h(a, a))) \vee \neg P(a, h(a, a), a) \vee \\ & \quad \neg P(g(a, k(h(a, a))), a, k(h(a, a))) \vee P(k(h(a, a)), h(a, a), k(h(a, a))) \\ & \big\} \end{aligned}$$

Poznámka 3.6.1 (Gilmore, 1960) *(:* Nech $S'_1, S'_2, \ldots$ sú možiny základných inštancií klauzúl z S. Gilmore vymyslel spôsob, ako generovať postupne $S'_1, S'_2, \ldots$ a aj spôsob, ako overovať ich nesplniteľnosť. Problém bol, že algoritmické metódy na zisťovanie nesplniteľnosti pracovali iba

pre menšie množiny klauzúl. S'_i bola totiž konjunkcia základných inštancií klauzúl z S. Lenže S je množina disjunkcií a dostaneme teda konjunktívnu normálnu formu. Túto formu bolo treba upraviť na disjunktívnu normálnu formu, pretože potom sa mohla optimalizovať metódami výrokovej logiky. Následne metóda vyhadzovala z DNF kontrárne dvojice. Pre veľa klauzúl krátkej dĺžky to znamenalo preberanie veľkého počtu možností. Ak máme 10 klauzúl každá dĺžky 2 literály, potrebujeme preverovať 2^{10} prípadov – zložitosť exponenciálne rastie. *:)*

Príklad 3.6.4 Majme množinu klauzúl $S = \{P(x),\ \neg P(a)\}$ a univerzum nech je $H_0 = \{a\}$. Ak zoberieme $S' = \{P(a), \neg P(a)\}$, máme $S'_0 = P(a) \wedge \neg P(a)$, čo sa dá upraviť na ε a teda S nie je splniteľná.

Príklad 3.6.5 Majme $S = \{P(a),\ \neg P(x) \vee Q(f(x)),\ \neg Q(f(a))\}$ a univerzum $H_0 = \{a\}$. . . . Dokázať nesplniteľnost množiny S možno nasledovne:

$$\begin{aligned} S'_0 &= P(a) \wedge [\neg P(a) \vee Q(f(a))] \wedge \neg Q(f(a)) \\ &= [P(a) \wedge \neg P(a) \wedge \neg Q(f(a))] \vee [P(a) \wedge Q(f(a)) \wedge \neg Q(f(a))] \\ &= \varepsilon \vee \varepsilon = \varepsilon \end{aligned}$$

3.6.1 Dokazovacie pravidlá

Zaviedli ich Martin Davis a Hilary Putnam ako súčasť ich algoritmu na automatické dokazovanie formúl. Z pravidiel ktoré si uvedieme bude najsilnejšie takzvané pravidlo rezu, pomocou ktorého sa dajú simulovať aj ostatné pravidlá.

Pravidlo tautológie

Nech S je množina klauzúl. Vynechajme z S všetky tautologické klauzuly. Množina S', ktorá nám zostane, nie je splniteľná práve vtedy, keď S nie je splniteľná.

Dôkaz: Keď S nie je splniteľné, tak ani S' nie je splniteľné – tautológie sú splnené pre ľubovoľné interpretácie. To, čo zostane, hovorí, či množina je alebo nie je splniteľná.
■

Pravidlo jednoliterálnych klauzúl

Nech S je množina klauzúl a L je nejaká jednoliterálová klauzula. Vynechajme z S všetky klauzuly, ktoré obsahujú literál L. Nech S' sú klauzuly, ktoré nám zostanú po vynechaní. Môžu nastať dva prípady:

1. $S' = \emptyset$. Potom množina klauzúl S je splniteľná – stačí zobrať model, ktorý obsahuje L.
2. $S' \neq \emptyset$. Vezmem si literál $\neg L$ a vynechám ho z z každej klauzuly, ktorá ho obsahuje.[7] Dostanem tak množinu klauzúl S''. Ak sa $\neg L$ nachádza v S', po vynechaní $\neg L$ dostaneme ε. Tvrdíme, že S'' nie je splniteľná $\iff$ S nie je splniteľná.

Dôkaz: Máme S', ktoré vzniklo vynechaním klauzúl obsahujúcich L z S. Ak $S' = \emptyset$, každá klauzula z S obsahuje L v disjunkcii (špeciálne L je tvaru $L \vee \varepsilon$). Stačí nám ohodnotenie, kedy L je pravdivé, čo zabezpečí pravdivosť celého výroku.

Keď S' nie je prázdna, vytvoríme S''. Ideme ukázať, že S'' nie je splniteľná práve vtedy, keď S nie je splniteľná.

$\Rightarrow$: Budeme dokazovať sporom. Predpokladajme, že S'' nie je splniteľná a S je splniteľná. Teda pre S existuje model $\mathcal{M}$ a tento musí obsahovať L. Lenže tým pádom v množine klauzúl S'' sú zbytky po vyhodení $\neg L$ splnené $\Rightarrow$ S'' je splniteľná – spor.

[7] Pozor, prechod od S k S' je principiálny iný ako prechod od S' ku S''. Prvý krát totiž mažeme celé klauzuly, zatiaľ čo druhýkrát iba literály v klauzulách.

$\Leftarrow$: Opačnú implikáciu budeme opäť dokazovať sporom. Nech S'' je splniteľná. Potom existuje model $\mathcal{M}''$ pre S''. Ak tomuto modelu pridám L, potom $\mathcal{M}'' \cup L$ je model pre S, čo je spor.

■

Pravidlo čistých literálov

Definícia 3.6.2 (Čistý literál) *Literál L základnej klauzuly z S budeme nazývať čistým, ak sa literál $\neg L$ nevyskytuje v žiadnej základnej klauzule S.*

Teraz môžeme sformulovať pravidlo:
Vezmime si z S literál L, ktorý je čistý a vynechajme z S všetky základné inštancie klauzúl obsahujúce L. Množinu, ktorá nám ostala označme ako S'. Tvrdíme, že S nie je splniteľná $\iff$ S' nie je splniteľná.

Dôkaz: S nie je splniteľná $\iff$ S' nie je splniteľná.

$\Rightarrow$: Budeme dokazovať sporom. Predpokladajme, že S nie je splniteľná. ale S' splniteľná je. Potom musí mať model $\mathcal{M}'$, ktorý jej vyhovuje a neobsahuje $L, \neg L$. Keď si vytvorím model $\mathcal{M} = \mathcal{M}' \cup L$, potom $\mathcal{M}$ je modelom pre S. Čiže S je splniteľná a to je spor.

$\Leftarrow$: Predpokladajme, že S' nie je splniteľná. Platí $S' \subseteq S$ a teda triviálne nie je splniteľná ani S.

■

Pravidlo rezu

Predpokladame, že množinu S vieme vyjadriť v tvare

$$(A_1 \vee L) \wedge \ldots \wedge (A_m \vee L) \quad \wedge \quad (B_1 \vee \neg L) \wedge \ldots \wedge (B_n \vee \neg L) \quad \wedge \quad R$$

pričom A_i, B_i, R neobsahujú L ani $\neg L$. Označme si množiny

$$S_1 = A_1 \wedge A_2 \wedge \ldots \wedge A_m \wedge R$$
$$S_2 = B_1 \wedge B_2 \wedge \ldots \wedge B_n \wedge R$$

Tieto množiny budeme tiež nazývať množiny rezu. Tvrdíme, že S nie je splniteľná $\iff$ $S_1 \vee S_2$ nie je splniteteľná, čo je to isté ako že S_1, S_2 nie sú splniteľné.

Dôkaz:

$\Rightarrow$: Dokazujme sporom. Nech $S_1 \vee S_2$ je splniteľná, teda aspoň jeden člen disjunkcie je splniteľný. Bunv nech je splniteľná množina S_1. Teda, máme pre ňu model $\mathcal{M}_1$. Keď pridáme modelu $\mathcal{M}_1$ klauzulu $\neg L$, dostávame model pre S.

$\Leftarrow$: Pre spor predpokladajme, že S je splniteľná. S má tým pádom model, označme ho $\mathcal{M}$. Model $\mathcal{M}$ obsahuje buď L alebo $\neg L$. Ak obsahuje L, $\mathcal{M}$ vyhovuje S_2. Naopak, ak obsahuje $\neg L$, model $\mathcal{M}$ vyhovuje S_1.[8]

■

Príklad 3.6.6 Majme množinu S vyjadrenú v tvare $S = (P \vee Q \vee \neg R) \wedge (P \vee \neg Q) \wedge \neg P \wedge R \wedge U$. Ukážeme, že množina klauzúl nie je splniteľná.

- $S = (P \vee Q \vee \neg R) \wedge (P \vee \neg Q) \wedge \neg P \wedge R \wedge U$.
- $(Q \vee \neg R) \wedge \neg Q \wedge R \wedge U$ – použili sme pravidlo jednoliterálových klauzúl (PJK) pre $\neg P$.

[8] Na prednáške boli vymenené S_1, S_2. Som si však takmer istý, že správny dôkaz je tento.

- $\neg R \wedge R \wedge U$ – použili sme PJK pre $\neg Q$.
- $\varepsilon \wedge U$ – použili sme PJK pre R. Je dôležité, že klauzulu $\neg R = \varepsilon \vee \neg R$ sme nemohli škrtnúť úplne, ostalo nám po nej ε.
- $\varepsilon \wedge \ldots$ je vždy nesplniteľné a teda S nie je splniteľná

Príklad 3.6.7 Uvažujme $S = (P \vee Q) \wedge \neg Q \wedge (\neg P \vee Q \vee \neg R)$. Ukážte, že množina klauzúl S je splniteľná.

- $S = (P \vee Q) \wedge \neg Q \wedge (\neg P \vee Q \vee \neg R)$.
- $P \wedge (\neg P \vee \neg R)$ – PJK pre $\neg Q$.
- $\neg R$ – PJK pre P.
- Uvažujme interpretáciu $I = \{P, \neg Q, \neg R\}$. S je splniteľná pri interpretácii I.

Príklad 3.6.8 Nech je $S = (P \vee Q) \wedge (P \vee \neg Q) \wedge (R \vee Q) \wedge (R \vee \neg Q)$. Ukážte, že S je splniteľná.

- $S = (P \vee Q) \wedge (P \vee \neg Q) \wedge (R \vee Q) \wedge (R \vee \neg Q)$.
- $(R \vee Q) \wedge (R \vee \neg Q)$ – pravidlo čistých literálov pre P
- $\neg\varepsilon$ – PČL pre R. Je dôležité si všimnúť, že nám ostalo splniteľné $\neg\varepsilon$ a nie ε.
- Pre interpretáciu $I = \{R, P\}$ je množina S splnená.

Príklad 3.6.9 Uvažujme $S = (P \vee \neg Q) \wedge (\neg P \vee Q) \wedge (Q \vee \neg R) \wedge (\neg Q \vee \neg R)$. Zistite, či množina je alebo nie je splniteľná.

- vytvoríme si množiny podľa pravidla rezu:

  $$(P \wedge \neg Q) \wedge (Q \vee \neg R) \wedge (\neg Q \vee \neg R)$$
  $$(\neg P \vee Q) \wedge (Q \vee \neg R) \wedge (\neg Q \vee \neg R)$$

  A dostávame množiny rezu

  $$S_1 = \neg Q \wedge (Q \vee \neg R) \wedge (\neg Q \vee \neg R)$$
  $$S_2 = Q \wedge (Q \vee \neg R) \wedge (\neg Q \vee \neg R)$$

- Na množinu S_1 použijeme PJK s literálom $\neg Q$ a dostávame $\neg R \wedge \neg R$.
- Podobne, ak na množinu S_2 použijeme PJK s Q, opäť dostávame $\neg R \wedge \neg R$.
- $\neg R \wedge \neg R$ je splniteľná a preto je celá množina S splniteľná.

Príklad 3.6.10 Majme $S = (P \vee Q) \wedge (P \vee \neg Q) \wedge (R \vee Q) \wedge (R \vee \neg Q)$.

- P je čistý literál, použijeme PČL: $(R \vee Q) \wedge (R \vee \neg Q)$.
- R je čistý literál a dostávame prázdny splniteľný výraz $\neg\varepsilon$

3.7 Metóda rezolvent pre výrokovú logiku

Definícia 3.7.1 (Rezolventa) *Nech C_1 a C_2 sú ľubovoľné klauzuly, L_1 je literál z C_1, L_2 je literál z C_2 a literály L_1, L_2 sú navzájom kontrárne. Vynechajme L_1 z C_1 a L_2 z C_2, dostaneme tak klauzuly C_1', C_2'. Disjunkciu $C_1' \vee C_2'$ nazveme rezolventou klauzúl C_1 a C_2.*

Príklad 3.7.1 Majme $C_1 = P \vee R$ a $C_2 = \neg P \vee Q$. Uvažujme kontrárnu dvojicu $P, \neg P$. Potom $C_1' = R$, $C_2' = Q$. Rezolventa je $R \vee Q$.

Príklad 3.7.2 Majme $C_1 = \neg P \vee Q \vee R$, $C_2 = \neg Q \vee S$. Kontrárna dvojica je $\neg Q$, Q a rezolventa $\neg P \vee R \vee S$.

Príklad 3.7.3 Majme klauzuly $C_1 : \neg P \vee Q$ a $C_2 : \neg P \vee R$. Tieto klauzuly nemajú rezolventu.

Veta 3.7.1 *Nech C_1 a C_2 sú klauzuly a nech C je ich rezolventa. Potom C je logickým dôsledkom klauzúl C_1 a C_2.*

Dôkaz: Nech $C_1 = L \vee C_1'$, $C_2 = \neg L \vee C_2'$ a $C = C_1' \vee C_2'$. Máme ukázať, že z pravdivosti C_1, C_2 vyplýva pravdivosť C.

Uvažujme interpretáciu I takú, že C_1 a C_2 sú v nej pravdivé. Rozoberieme si 2 možnosti:

- L nie je pravdivý literál v I. Potom musí platiť, že C_1' je pravdivý v I. Tým pádom je ale aj C pravdivé v I.
- $\neg L$ nie je pravdivý literál v I. Potom je evidentne klauzula C_2' pravdivá v I. A zo toho vyplýva, že aj C je pravdivé v I.

■

Poznámka 3.7.1 *(:* Nech C_1, C_2 sú jednotkové klauzuly. Ak C_1, C_2 majú rezolventu, potom musia tvoriť kontrárnu dvojicu $L, \neg L$ a rezolventou je prázdna (nesplniteľná) klauzula $C \equiv \varepsilon$. *:)*

Našim cieľom bude zovšeobecniť predchádzajúcu poznámku do nasledujúceho variantu: Nech S je množina klauzúl. Potom S je nesplniteľná práve vtedy keď z nej vieme nejakým spôsobom pomocou rezolvent získať prázdnu klauzulu. Teraz si to formálne rozpíšeme.

Definícia 3.7.2 (Rezolvenčné odvodenie) *Nech S je množina klauzúl. Rezolvenčným odvodením klauzuly C z množiny klauzúl S nazývame konečnú postupnosť klauzúl $C_1, C_2, \ldots, C_n$ (kde $C_n \equiv C$) takú, že pre každé $i \in \{1, 2, \ldots, n\}$ platí: C_i je buď z S alebo C_i je rezolventa niektorých klauzúl C_j, C_k pre $j, k < i$.*

Ak C je prázdna klauzula, potom takémuto odvodeniu hovoríme zamietnutie odvodenia alebo tiež dôkaz nesplniteľnosti S.

Definícia 3.7.3 *Majme množinu klauzúl S a klauzulu C. Hovoríme, že C môžeme získať z S, ak existuje (rezolvenčné) odvodenie $C_1, \ldots, C_m$ z množiny S také, že $C_m \equiv C$.*

Príklad 3.7.4 Uvažujme množinu klauzúl $S = \{\neg P \vee Q,\ \neg Q,\ P\}$. Uvažujme nasledujúce rezolvenčné odvodenie

1: $\neg P \vee Q$ – z S

2: $\neg Q$ – z S

3: $\neg P$ – pravidlo rezolventy na 1,2

4: P – z S.

5: ε – pravidlo rezolventy na 3,4

Dostali sme prázdnu klauzulu a teda množina klauzúl S nie je splniteľná.

Príklad 3.7.5 Nech $S = \{P \vee Q,\ \neg P \vee Q,\ P \vee \neg Q,\ \neg P \vee \neg Q\}$. Opäť vieme dokázať nesplniteľnosť množiny klauzúl S:

1: $P \vee Q$ – z S

2: $\neg P \vee Q$ – z S

3: $P \vee \neg Q$ – z S

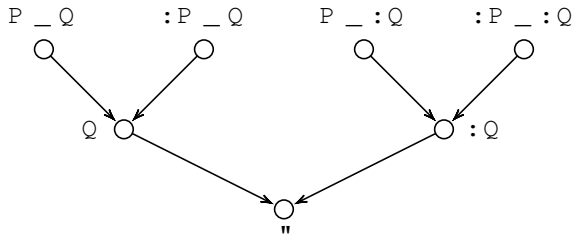
4: $\neg P \vee \neg Q$ – z S

5: Q – rezolventa 1,2

6: $\neg Q$ – rezolventa 3,4

7: ε – rezolventa 5,6

K tomuto odvodeniu môžeme navyše nakresliť aj jeho strom (obr. 3.8).



Obr. 3.8: Strom rezolvenčného odvodenia z príkladu 3.7.5

Poznámka 3.7.2 *(:* Pravidlom rezolventy smerujeme k tomu, že sa snažíme získať prázdnu klauzulu. Dôležité je, že je to silné pravidlo, t.j., že ak je množina S nie je splniteľná, vieme prázdnu klauzulu naozaj odvodiť iba pomocou tohoto pravidla. Na začiatok začneme ekvivalenciou pravidla rezolventy a pravidla modus ponens. *:)*

Lema 3.7.1 *Pravidlo modus ponens je ekvivalentné s pravidlom rezolventy.*

Dôkaz: Najskôr si ukážeme, že pomocou MP vieme dokázať pravidlo rezolventy: Chceme ukázať $A \to B, \neg A \to C \vdash \neg B \to C$. Postupujme nasledovne:

1. $\vdash (A \to B) \to (\neg B \to \neg A)$ – tvrdenie z výrokovej logiky
2. $A \to B \vdash A \to B$
3. $A \to B \vdash \neg B \to \neg A$ – MP 1,2
4. $\vdash (\neg B \to \neg A) \to ((\neg A \to C) \to (\neg B \to C))$ – jednoduchý sylogizmus.
5. $A \to B \vdash (\neg A \to C) \to (\neg B \to C)$ – MP 3,4
6. $\neg A \to C \vdash \neg A \to C$
7. $A \to B, \neg A \to C \vdash \neg B \to C$ – MP 5,6

Poznamenajme pritom, že obidve využité tvrdenia výrokovej logiky sa dajú dokázať z axióm iba pomocou pravidla modus ponens.

Naopak, uvažujme, že chceme pravidlo MP simulovať pomocou pravidla rezolventy. Teda chceme ukázať $A, A \to B \vdash B$. Použijeme nasledujúci trik:

1. $A \equiv A \vee \varepsilon$
2. $A \to B \equiv \neg A \vee B$
3. $A \vee \varepsilon, \neg A \vee B \vdash \varepsilon \vee B$ – použijeme pravidlo rezolventy na ekvivalentné zápisy formúl $A, A \to B$
4. $B \equiv \varepsilon \vee B$ a teda
5. $A, A \to B \vdash B$.

■

3.8 Substitúcia a unifikácia

Vo výrokovej logike nebol problém hľadať kontrárne dvojice. Zložitejšia situácia ale nastáva v prípade predikátovej logiky prvého rádu. A práve tomu sa budeme venovať v tejto kapitole. Uvažujme napríklad dve klauzuly $C_1 = P(x) \vee Q(x)$, $C_2 = \neg P(f(x)) \vee R(x)$. V nich neexistuje žiadna kontrárna dvojica. Ak však nahradím premennú x za term $f(a)$ v prvej klauzule a za term a v druhej klauzule, dostaneme základné inštancie $C_1' = P(f(a)) \vee Q(f(a))$, $C_2' = \neg P(f(a)) \vee R(a)$. Teraz môžeme definovať rezolventu; bude to $Q(f(a)) \vee R(a)$. Mohli by sme postupovať aj všeobecnejšie – nahraďme x za $f(x)$ v prvej klauzule a dostávame $C_1^* = P(f(x)) \vee Q(f(x))$, $C_2^* = \neg P(f(x)) \vee R(x)$.

Rezolventa potom bude $C^* = Q(f(x)) \vee R(x)$. Vidíme teda, že sme získali 2 rôzne rezolventy, jednu viac všeobecnú ako druhú. No a práve v ďalšom texte si formálne zadefinujeme toto dosadzovanie hodnôt a popíšeme spôsob, ako hľadať najvšeobecnejšie rezolventy.

Definícia 3.8.1 (Substitúcia) *Pod substitúciou rozumieme konečnú množinu tvaru: $\{t_1/v_1, \ldots, t_n/v_n\}$, kde každé v_i je premenná a t_i je term. Ďalej požadujeme, aby všetky v_i boli navzájom rôzne ($i \in \{1, \ldots, n\}$) a aby term t_i bol rôzny od v_i. Touto množinuo budeme popisovať činnosť "naraz nahraď každú premennú v_i termom t_i".*

Ak $t_1, \ldots, t_n$ sú základné inštancie (teda termy bez premenných), tak substitúciu nazývame tiež základná substitúcia.

Poznámka 3.8.1 *(:* Na označovanie substitúcií budeme používať grécke písmená. Špeciálne, prázdnu substitúciu označíme ako ε.[9] *:)*

Poznámka 3.8.2 *(:* Je dôležité si všimnúť, že poradie prvkov v definícii substitúcie je čisto antiintuitívne – človek by očakával "premenná/výraz ktorým ju máme nahradiť" a nie "výraz/premenná". *:)*

Príklad 3.8.1 Jedna substitúcia môže byť napr. $\alpha = \{f(z)/x,\ y/z\}$, teda x nahrádzame za $f(z)$ a z za y. Ďalšia môže byť $\beta = \{a/x,\ g(y)/y,\ f(g(y))/z\}$.

Definícia 3.8.2 *Nech θ je ľubovoľná substitúcia a E je nejaký výraz. Nech $\theta = \{t_1/v_1, \ldots, t_n/v_n\}$. Potom $E\theta$ označuje výraz, ktorý vznikne tak, že súčasne vo výraze E nahradíme každý výskyt premenej v_i termom t_i pre $i \in \{1, \ldots, n\}$. Takýto výraz nazveme inštanciou E.*

Príklad 3.8.2 Majme substitúciu $\theta = \{a/x,\ f(b)/y,\ c/z\}$ a výraz $E = P(x, y, z)$. Potom $E\theta = P(a, f(b), c)$.

Ďalšia operácia, ktorú budeme potrebovať, je operácia skladania substitúcií.

[9] Pozn.: Vzniká nám tu kolízia označenia s prázdnou nesplniteľnou klauzulou. Z kontextu však bude jasné, o ktorý prípad pôjde.

Definícia 3.8.3 (Kompozícia substitúcii) *Majme substitúcie* $\theta = \{t_1/x_1, \dots t_n/x_n\}$ *a* $\lambda = \{u_1/y_1, \dots u_m/y_m\}$. *Zloženie (kompozícia)* $\theta \circ \lambda$ *substitúcií* θ, λ *je definované ako množina*

$$\{t_1\lambda/x_1, \dots, t_n\lambda/x_n, u_1/y_1, \dots, u_m/y_m\}$$

z ktorej navyše vyradíme všetky členy $t_i\lambda/x_i$, *pre ktoré platí, že* $t_i\lambda = x_i$ *(aby sme nesubstituovali identititami) a tiež vyradíme všetky* u_i/y_i, *pre ktoré* $y_i \in \{x_1, x_2, \dots, x_n\}$ *(lebo by sme mali dvojité správanie sa substitúcie na* x_i*).*

Poznámka 3.8.3 *(:* Kompozícia $\theta \circ \lambda$ sa správa rovnako ako postupné aplikovanie θ, λ. Čiže $E(\theta \circ \lambda) = (E\theta)\lambda$. *:)*

Príklad 3.8.3 Majme substitúcie

$$\theta = \{t_1/x_1,\ t_2/x_2\} = \{f(y)/x,\ z/y\}$$
$$\lambda = \{u_1/y_1,\ u_2/y_2,\ u_3/y_3\} = \{a/x,\ b/y,\ y/z\}$$

Potom

$$\begin{aligned}\theta \circ \lambda &= \{t_1\lambda/x_1,\ t_2\lambda/x_2,\ u_1/y_1,\ u_2/y_2,\ u_3/y_3\} - \{\dots\} \\ &= \{f(b)/x,\ y/y,\ a/x,\ b/y,\ y/z\} - \{y/y,\ a/x,\ b/y\} \\ &= \{f(b)/x,\ y/z\}\end{aligned}$$

Poznámka 3.8.4 *(:* Skladanie substitúcií je asociatávna operácia, teda ak zoberieme θ, λ, μ, potom platí $\theta \circ (\lambda \circ \mu) = (\theta \circ \lambda) \circ \mu$.

Tiež platí, že $\varepsilon \circ \theta = \theta = \theta \circ \varepsilon$. To znamená, že množina substitúcii s operáciou skladania je pologrupa (monoid) s jednotkou. *:)*

Definícia 3.8.4 (Unifikátor) *Substitúciu* θ *nazveme unifikátorom množiny výrazov* $E_1, E_2, \dots, E_n$, *ak platí* $E_1\theta = E_2\theta = \dots = E_n\theta$. *Množinu nazveme unifikovateľnou, ak pre ňu existuje unifikátor, ktorý je zjednocuje.*

Príklad 3.8.4 Majme množinu $\{P(a, y),\ P(x, f(b)\}$. Potom jeden z možných unifikátorov je napríklad $\theta = \{a/x,\ f(b)/y\}$.

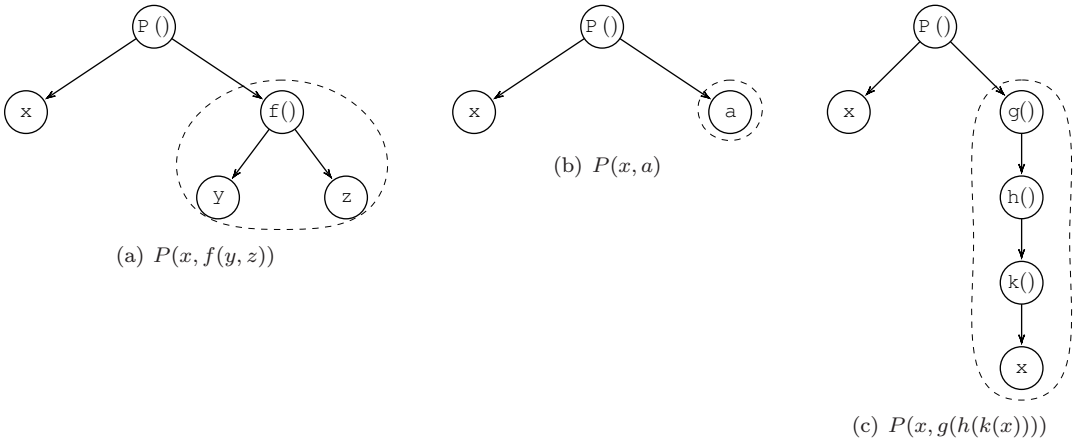
Poznámka 3.8.5 *(:* Nie každá množina má unifikátor. Naopak, množina môže mať aj viacej unifikátorov. Vtedy má medzi nimi význačné miesto takzvaný najvšeobecnejší unifikátor. *:)*

Definícia 3.8.5 (Najvšeobecnejší unifikátor) *Majme množinu výrazov* $S = \{E_1, E_2, \dots, E_n\}$. *Unifikátor* σ *pre množinu výrazov* S *nazveme najvšeobecnejší unifikátor, ak pre ľubovoľný unifikátor* θ *množiny* S *platí, že existuje substitúcia* λ_θ *taká, že* $\theta = \sigma \circ \lambda_\theta$.

Pri hľadaní unifikátorov budeme pozerať na rozdiely vo výrazoch. Uvažujme napríklad výrazy $P(a), P(x)$. Pozerajme sa na ne ako na konečnú postupnosť symbolov – odlišujú sa akurát v treťom symbole. Toto je prvá odlišnosť/diferencia. Vo všeobecnosti môže byť týchto výrazov viacej a preto si zadefinujeme diferenčnú množinu.

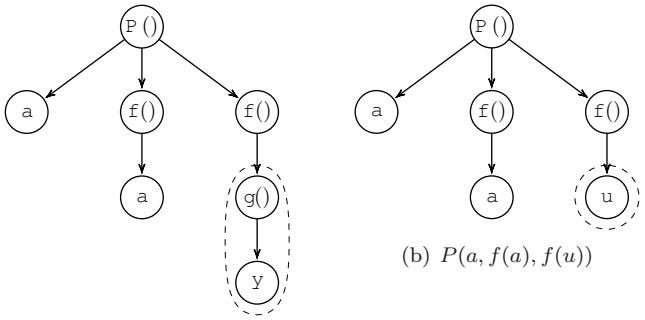
Definícia 3.8.6 (Diferenčná množina) *Nech* W *je neprázdna množina výrazov. Diferenčnú množinu pre množinu výrazov* W *dostávame tak, že na výrazy sa pozrieme ako na postupnosti symbolov, nájdeme prvú pozíciu (zľava), na ktorej sa líšia a tieto rozdielne výrazy vypíšeme.*

Poznámka 3.8.6 (Nebolo na prednáške) *(:* Iný (a podľa mňa lepší) pohľad na to, ako získať diferenčnú množinu je pozrieť sa na stromy daných výrazov a začať ich naraz rekurzívne prehľadávať zľava doprava až narazíme na vrchol, ktorý je v niektorom výraze iný. Vtedy do diferenčnej množiny zoberieme pre každý výraz podstrom zakorenený v dotyčnom vrchole. *:)*



(a) $P(x, f(y, z))$ (b) $P(x, a)$ (c) $P(x, g(h(k(x))))$

Obr. 3.9: Ukážka diferenčnej množiny z príkladu 3.8.5



(a) $P(a, f(a), f(g(y)))$ (b) $P(a, f(a), f(u))$

Obr. 3.10: Ukážka diferenčnej množiny z príkladu 3.8.6

Príklad 3.8.5 Majme množinu $W = \{P(x, f(y, z),\ P(x, a),\ P(x, g(h(k(x))))\}$. Nájdeme prvý pozíciu na ktorej sa líšia: $\{P(x, \underline{f(y, z)},\ P(x, \underline{a}),\ P(x, \underline{g(h(k(x))))})\}$. Diferenčnou množinou bude množina líšiacich sa podvýrazov, teda $D = \{\underline{f}(y, z),\ \underline{a},\ \underline{f(h(k(x)))}\}$. Jej grafická konštrukcia je na obrázku 3.9.

Príklad 3.8.6 (Nebol na prednáške) Uvažujme $W = \{P(a, f(a), f(g(y))),\ P(a, f(a), f(u))\}$. Diferenčná množina je $D = \{g(y), u\}$ a grafické znázornenie je na obrázku 3.10.

Poznámka 3.8.7 *(:* Do diferenčnej množiny zakaždým vyberáme iba jednu (prvú) nezhodu. Napríklad pre $W = \{P(x, y, z),\ P(y, f(a), g(x, y))\}$ je diferenčná množina iba $D = \{x, y\}$. *:)*

3.8.1 Unifikačný algoritmus

Teraz si ukážeme jeden z algoritmov používaných na unifikáciu množiny. Bude dookola opakovať nasledujúce kroky:

1. na začiatku polož kolo $k = 0$, množinu na unifikovanie $W_0 = W$ a počiatočnú substitúciu $\sigma_0 = \varepsilon$.
2. Ak W_k obsahuje jedinú klauzulu,[10] algortimus zakončí svoju činnosť a σ_k je najvšeobecnejší unifikátor. V opačnom prípade nájdeme diferenčnú množinu D_k pre W_k.

[10]Na prednáške to bolo "obsahuje jednotkovú klauzulu" ale toto označenie je mätúce.

3. Ak existujú také elementy $v_k, t_k \in D_k$, že v_k je premenná, ktorá sa nevyskytuje v terme t_k, tak pokračujeme ďalším krokom. V opačnom prípade algoritmus zakončuje svoju činnosť s výsledkom, že množina W nie je unifikovateľná.

4. Položme $W_{k+1} = W_k\{t_k/v_k\}$ a $\sigma_{k+1} = \sigma_k \circ \{t_k/v_k\}$.

5. pokračujeme krokom 2.

Poznámka 3.8.8 *(:* Ak je množina unifikovateľná, vždy existuje najvšeobecnejší unifikátor. *:)*

Príklad 3.8.7 Nájdite najvšeobecnejší unifikátor pre množinu

$$W = \{P(a, x, f(g(y))),\ P(z, f(z), f(u))\}$$

Algoritmus bude pracovať nasledovne:

1. $\sigma_0 = \varepsilon, W_0 = W$.

2. Pretože W_0 obsahuje viac klauzúl klauzula, σ_0 nie je najvšeobecnejší unifikátor a pokračujeme vo výpočte.

3. Zostrojíme diferenčnú množinu $D_0 = \{a, z\}$. Existuje premenná $v_0 = z$, ktorá nie je obsiahnutá v terme $t_0 = a$.

4.
$$\sigma_1 = \sigma_0 \circ \{t_0/v_0\} = \varepsilon \circ \{a/z\} = \{a/z\}$$
$$\begin{aligned} W_1 &= W_0\{t_0/v_0\} = \{P(a, x, f(g(y))),\ P(z, f(z), f(u))\}\{a/z\} \\ &= \{P(a, x, f(g(y))),\ P(a, f(a), f(u))\} \end{aligned}$$

5. W_1 neobsahuje jedinú klauzulu. Pokračujeme vo výpočte

6. Zostrojíme diferenčnú množinu $D_1 = \{x, f(a)\}$.

7. V D_1 máme premennú $v_1 = x$ a term $t_1 = f(a)$.

8.
$$\sigma_2 = \sigma_1 \circ \{t_1/v_1\} = \{a/z\} \circ \{f(a)/x\} = \{a/z,\ f(a)/x\}$$
$$\begin{aligned} W_2 &= W_1\{t_1/v_1\} = \{P(a, x, f(g(y))),\ P(a, f(a), f(u))\}\{f(a)/x\} = \\ &= \{P(a, f(a), f(g(y))),\ P(a, f(a), f(u))\} \end{aligned}$$

9. W_2 nie je jednotková klauzula – vytvárame diferenčnú množinu $D_2 = \{g(y), u\}$.

10. $v_2 = u$, $t_2 = g(y)$.

11.
$$\sigma_3 = \sigma_2 \circ \{t_2/v_2\} = \{a/z, f(a)/x\} \circ \{g(y)/u\} = \{a/z,\ f(a)/x,\ g(y)/u\}$$
$$\begin{aligned} W_3 &= W_2\{t_x/v_2\} = \{P(a, f(a), f(g(y))),\ P(a, f(a), f(u))\}\{g(y)/u\} = \\ &= \{P(a, f(a), f(g(y))),\ f(a, f(a), f(g(y))\} \end{aligned}$$

12. W_3 obsahuje iba jedinú klauzulu a teda σ_3 je najvšeobecnejší unifikátor pre množinu klauzúl W.

Príklad 3.8.8 Zistite, či je unifikovateľná množina

$$W = \{Q(f(a), g(x)),\ Q(y, y)\}$$

1. $\sigma_0 = \varepsilon$, $W_0 = W$.
2. W_0 obsahuje viac klauzúl. Nájdeme diferenčnú množinu $D_0 = \{f(a), y\}$.
3. $v_1 = y$, $t_1 = f(a)$.
4. $\sigma_1 = \sigma_0 \circ \{t_0/v_0\} = \varepsilon \circ \{f(a)/y\} = \{f(a)/y\}$.
5. $W_1 = W_0\{t_0/\sigma_0\} = \{Q(f(a), g(x)),\ Q(f(a), f(a))\}$.
6. W_1 obsahuje 2 klauzuly, zostrojujeme $D_1 = \{g(x), f(a)\}$.
7. V D_1 nemáme prvok, ktorý by bol premennou. Algoritmus ukončí svoju činnosť s výsledkom, že W nie je unifikovateľná.

Poznámka 3.8.9 *(:* Pri zisťovaní unifikovateľnosti vždy vytvárame množiny W_i tvaru

$$W\sigma_0, W\sigma_1, W\sigma_2, \ldots$$

pričom v každom kroku sa zmenší počet premenných aspoň o 1. Po konečnom počte krokov sa teda algoritmus musí zastaviť. *:)*

Veta 3.8.1 (Unifikačná) *Ak W je konečná neprázdna unifikovateľná množina výrazov, tak unifikačný algoritmus vždy zakončuje svoju činnosť na druhom kroku a posledné σ_k je najvšeobecnejší unifikátor.*

Dôkaz: Nech W je unifikovateľná množina a nech Θ označuje jej ľubovoľný unifikátor. Označme si počet kôl algoritmu ako n.

Indukciou ukážeme, že pre každé kolo k počas výpočtu programu existuje taká substitácia λ_k, že $\Theta = \sigma_k \circ \lambda_k$.

- Báza indukcie: Nech $k = 0$. Máme ukázať, že existuje λ_0, pre ktorú platí $\Theta = \sigma_0 \circ \lambda_0$. V tomto prípade $\sigma_0 = \varepsilon$ a teda $\lambda_0 = \Theta$.
- Indukčný krok: Predpokladáme, že existuje λ_k, pre ktoré platí $\Theta = \sigma_k \circ \lambda_k$. Pozrime sa na množinu $W_{k+1} = W\sigma_{k+1}$.

  Ak W_k je jednotková klauzula, tak algoritmus zakončuje svoju činnosť na druhom kroku a σ_k je najvšeobecnejší unifikátor pre W.

  Nech teda W_k nie je jednotková množina. Potom hľadáme diferenčnú množinu D_k pre množinu W_k. D_k je diferenčná množina pre W_k a vo W_k musí existovať premenná – označme ju v_k. Ďalej musí existovať term t_k rôzny od v_k. Ak by toto neplatilo, tak množina by nemohla byť unifikovateľná.[11]

  Vieme, že diferenčnú množinu D_k unifikuje substitúcia λ_k. Teda $v_k\lambda_k = t_k\lambda_k$.

  Ďalej budeme potrebovať, že v_k nie je obsiahnuté v t_k. Ak by totiž premenná v_k bola obsiahnutá v t_k, dôjdeme k sporu. Platilo by aj "$v_k\lambda_k$ je obsiahnutá v $t_k\lambda_k$". Lenže vieme, že tam platí rovnosť a preto by musela platiť aj rovnosť $v_k = t_k$. Spor.

  Vypočítame $\sigma_{k+1} = \sigma_k \circ \{t_k/v_k\}$. Potrebovali by sme nájsť λ_{k+1}. Môžeme si ho napríklad "tipnúť" ako $\lambda_{k+1} = \lambda_k - \{t_k\lambda_k/v_k\}$.

  Pretože v_k sa nevyskytuje v t_k, platí $t_k\{t_k\lambda_k/v_k\} = \varepsilon$ a tým pádom

$$t_k\lambda_{k+1} = t_k(\lambda_k - \{t_k\lambda_k/v_k\}) = t_k\lambda_k$$

[11] Náhľad prečo: Vieme, že $\Theta = \sigma_k \circ \lambda_k$ a pre λ_k musí nutne unifikovať diferenčnú množinu D_k. Tým pádom aspoň jedna z "jednotkových substitúcii" v λ_k musí obsahovať elementy z D_k.

A teda dostávame

$$\begin{aligned}\{t_k/v_k\} \circ \lambda_{k+1} &= \{t_k\lambda_{k+1}/v_k\} \cup \lambda_{k+1} \\ &= \{t_k\lambda_k/v_k\} \cup \lambda_{k+1} \\ &= \{t_k\lambda_k/v_k\} \cup (\lambda_k - \{t_k\lambda_k/v_k\}) \\ &= \lambda_k\end{aligned}$$

Výsledok je teda, že $\lambda_k = \{t_k/v_k\} \circ \lambda_{k+1}$, čiže $\Theta = \sigma_k \circ \lambda_k = \sigma_k \circ \{t_k/v_k\} \circ \lambda_{k+1} = \sigma_{k+1} \circ \lambda_{k+1}$. A to sme chceli ukázať.

■

3.9 Metóda rezolvent pre logiku 1. rádu

Definícia 3.9.1 (Spojenie) *Nech C je klauzula, ktorá obsahuje dva alebo viac literálov (a tie pozostávajú z rovnakého predikátu len s inými parametrami). Ak tieto literály majú najvšeobecnejší unifikátor σ, tak $C\sigma$ sa nazývame spojením C.*

Ak $C\sigma$ je jednotková klauzula, tak $C\sigma$ nazývame tiež jednotkovým spojením C.

Príklad 3.9.1 Uvažujme klauzulu C, ktorá vyzerá nasledovne: $C = \{P(x) \vee P(f(y)) \vee \neg Q(x)\}$. Zoberme literály $P(x)$ a $P(f(y))$. Ich najvšeobecnejší unifikátor je $\sigma = \{f(y)/x\}$. Potom spojenie je $C\sigma = \{P(f(y)) \vee \neg Q(x)\}$.

Definícia 3.9.2 (binárna rezolventa) *Nech C_1 a C_2 sú dve klauzuly (budeme ich nazývať predpoklady), ktoré nemajú spoločné premenné. Nech $L_1 \in C_1$ a $L_2 \in C_2$ sú dva literály. Ak L_1 a $\neg L_2$ majú najvšeobecnejší unifikátor σ, tak výraz*

$$(C_1\sigma - L_1\sigma) \cup (C_2\sigma - L_2\sigma)$$

sa nazýva binárnou rezolventou.[12] *Literály L_1 a L_2 môžeme vynechať a nazývame ich nadbytočné.*

Príklad 3.9.2 Majme $C_1 = P(x) \vee Q(x)$ a $C_2 = \neg P(a) \vee R(x)$, čo budú predpoklady. Na to, aby sme mohli previesť operáciu binárnej rezolventy, musíme najskôr premenovať premenné v druhom výraze, aby boli rôzne od tých v prvom. Máme teda $C_2' = \neg P(a) \vee R(y)$.

Uvažujme teraz klauzuly $L_1 = P(x)$ a $L_2 = \neg P(a)$. Ich najvšeobecnejší unifikátor je $\sigma = \{a/x\}$.

Binárna rezolventa C_1 a C_2 je

$$\begin{aligned}(C_1\sigma - L_1\sigma) \cup (C_2\sigma - L_2\sigma) &= (\{P(a),\ Q(a))\} - \{P(a)\}) \cup (\{\neg P(a),\ R(y)\} - \{\neg P(a)\}) \\ &= Q(a) \vee R(y)\end{aligned}$$

Nadbytočné literály sú $P(x), \neg P(a)$.

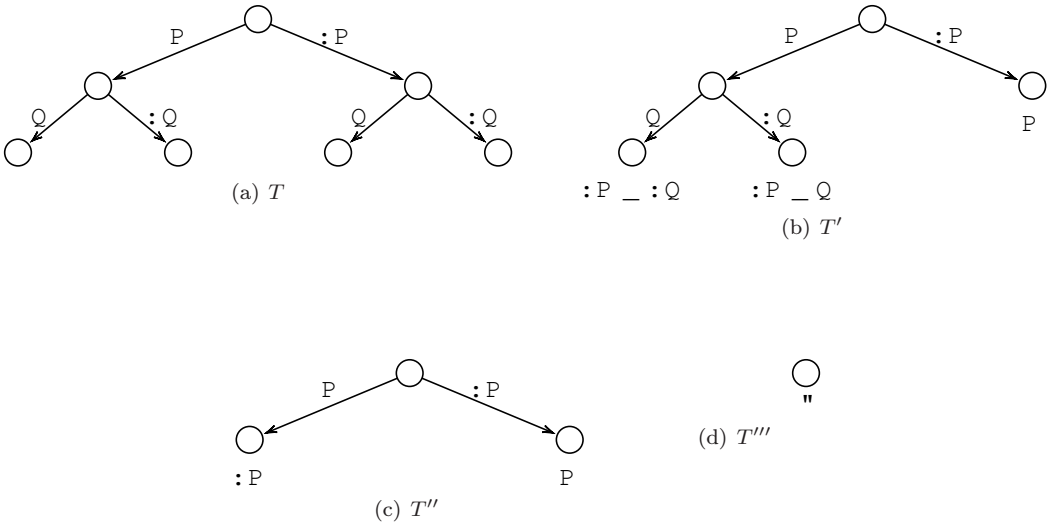
Definícia 3.9.3 (Rezolventa logiky 1. rádu) *Rezolventou z predpokladov C_1 a C_2 definujeme ako jednu z nasledujúcich binárnych rezolvent:*

1. *Binárna rezolventa C_1 a C_2*
2. *Binárna rezolventa C_1 a spojenia C_2*
3. *Binárna rezolventa spojenia C_1 a C_2*
4. *Binárna rezolventa spojenia C_1 a spojenia C_2*

Príklad 3.9.3 Uvažujme $C_1 = P(x) \vee P(f(y)) \vee R(g(y))$, $C_2 = \neg P(f(g(a)) \vee Q(b)$.

Spojenie C_1 je $C_1' : P(f(y)) \vee R(g(y))$. Binárna rezolventa C_1' a C_2 (a tým pádom rezolventa C_1, C_2) bude $R(g(g(a))) \vee Q(b)$.

[12] Za pozornosť stojí fakt, že vo všeobecnosti $(C\sigma - L\sigma) \neq (C - L)\sigma$.



Obr. 3.11: Stromy z príkladu 3.9.4

Ešte predtým, než sa plne vrhneme do dokazovania úplnosti metódy rezolvent, uvedieme si príklady na osvieženie pamäti.

Príklad 3.9.4 Majme množinu klauzúl $S = \{P,\ \neg P \vee Q,\ \neg P \vee \neg Q\}$. Prislúchajúca herbrandovská báza je $\{P, Q\}$. Množine klauzúl S zodpovedá úplný sémantický strom T naznačený na obrázku 3.11.

K úplnému stromu T môžeme zostrojiť uzavretý sémantický strom v ktorom každá vetva sa končí odmietajúcim vrcholom, teda odmieta niektorú z klauzúl z S. Vieme, že žiadna z tých interpretácií, ktoré končia v listoch, nie je splniteľná.

Následne, strom T' môžeme postupne pravidlom rezolventy upravovať – klauzuly $\neg P \vee \neg Q$, $\neg P \vee Q$ obsahujú kontrárnu dvojicu $\neg Q, Q$. Ich rezolventa je $\neg P$. Množinu S teda môžeme obohatiť a dostaneme $S'' = S \cup \{\neg P\}$. Môžeme tiež upraviť aj strom T' a dostávame T''.

Pokračujme ďalej: $P, \neg P$ sú kontrárna dvojica a ich rezolventou je ε. Dostávame strom T'''.

Dospeli sme teda k tomu, že množina klauzúl S je nesplniteľná. Zároveň si môžeme všimnúť, že každým aplikovaním pravidla rezolventy zmenšujeme strom.

Príklad 3.9.5 (Opakovanie z úvodu k substitúcii) Uvažujme dve klauzuly $C_1 = P(x) \vee Q(x)$, $C_2 = \neg P(f(x)) \vee R(x)$.

V nich neexistuje žiadna kontrárna dvojica. Nahradením x za $f(a)$ resp. a dostaneme základné inštancie $C_1' = P(f(a)) \vee Q(f(a))$, $C_2' = \neg P(f(a)) \vee R(a)$. Teraz môžeme vypočítať rezolventu $Q(f(a)) \vee R(a)$.

Mohli by sme postupovať aj všeobecnejšie – nahraďme x za $f(x)$ v prvej klauzule a dostávame $C_1^* = P(f(x)) \vee Q(f(x))$, $C_2^* = \neg P(f(x)) \vee R(x)$.

Rezolventa potom bude $C^* = Q(f(x)) \vee R(x)$. Vidíme teda, že sme získali 2 rôzne rezolventy, jednu viac všeobecnú ako druhú.

Úplnosť metódy rezolvent

Metódu rezolvent zaviedol roku 1965 Robinson. Táto metóda je omnoho efektívnejšia ako pravidlá, ktoré zaviedli Davis a Putnam. Veľmi dôležitým aspektom je hlavne to, že metóda je úplná: Ak množina klauzúl nie je splniteľná, potom metódou rezolvent z nej vždy môžeme dostať prázdnu klauzulu (a teda formula nie je splniteľná v žiadnej interpretácii).

Lema 3.9.1 *Nech C_1' a C_2' sú inštancie klauzúl C_1 resp. C_2. Ak C' je rezolventa C_1' a C_2', tak potom existuje rezolventa*[13] *C klauzúl C_1 a C_2, že C' je inštancia C.*

[13]Na prednáške to bolo prezentované takto. Je však evidentné, že to malo byť formulované "existuje rezolventa

Dôkaz: Ak je treba, ako prvý krok premenujeme premenné v C_1 a C_2 aby boli rôzne (samozrejme, rovnaké premenovanie spravíme aj v inštanciách C_1', C_2'). Nech teraz L_1' a L_2' sú literály v C_1', C_2', ktoré môžeme vynechať (sú nadbytočné). Zoberme ich najvšeobecnejší unifikátor ν a binárna rezolventa C' bude

$$C' = (C_1'\nu - L_1'\nu) \cup (C_2'\nu - L_2'\nu)$$

C_1', C_2' sú inštancie C_1 a C_2 a teda existuje substitúcia[14] Θ taká, že platí:

$$C_1' = C_1\Theta$$
$$C_2' = C_2\Theta$$

Označme si teraz literály z C_i, ktoré zodpovedajú po substituovaní substitúciou Θ literálu L_i' ako $L_i^1, L_i^2, \ldots, L_i^{r_i}$ kde $i = 1, 2$. Teda platí

$$L_i^1\Theta = L_i^2\Theta = \cdots = L_i^{r_i}\Theta = L_i'$$

Ďalej si označme najvšeobecnejší unifikátor pre $\{L_i^1, L_i^2, \ldots, L_i^{r_i}\}$ ako λ_i. Platí

$$L_i^1\lambda_i = L_i^2\lambda_i = \cdots = L_i^{r_i}\lambda_i = L_i.^{15}$$

Pretože λ_i je najvšeobecnejší unifikátor, pre vhodnú substitúciu ξ platí:

$$L_i' = L_i^j\Theta = L_i^j(\lambda_i \circ \xi) = (L_i^j\lambda_i)\xi = L_i\xi$$

Pre pohodlnosť označme $\lambda = \lambda_1 \cup \lambda_2$. Z predpokladov vety je jasné, že $L_1', \neg L_2'$ sú unifikovateľné. Označme ich najvšeobecnejší unifikátor ako σ. Teraz pozor, zamerajme sa na spojenie $C_1\lambda_1$ a $C_2\lambda_2$. Hľadanú najvšeobecnejšiu rezolventu zostrojíme práve pomocou nich:

$$\begin{aligned} C &= ((C_1\lambda)\sigma - L_1\sigma) \cup ((C_2\lambda_2)\sigma - L_2\sigma) \\ &= ((C_1\lambda)\sigma - (\{L_1^1, L_1^2, \ldots, L_1^{r_1}\}\lambda)\sigma) \cup ((C_2\lambda)\sigma - (\{L_2^1, L_2^2, \ldots, L_2^{r_2}\}\lambda)\sigma) \\ &= (C_1(\lambda \circ \sigma) - \{L_1^1, \ldots, L_1^{r_1}\}(\lambda \circ \sigma)) \cup (C_2(\lambda \circ \sigma) - \{L_2^1, \ldots, L_1^{r_2}\}(\lambda \circ \sigma)) \end{aligned}$$

Na záver ešte potrebujeme overiť, že C' je inštancia C.

$$\begin{aligned} C' &= (C_1'\nu - L_1'\nu) \cup (C_2'\nu - L_2'\nu) \\ &= ((C_1\Theta)\nu - (\{L_1^1, \ldots, L_1^{r_1}\}\Theta)\nu) \cup ((C_2\Theta)\nu - (\{L_2^1, L_2^2, \ldots, L_2^{r_2}\}\Theta)\nu) \\ &= (C_1(\Theta \circ \nu) - \{L_1^1, \ldots, L_1^{r_1}\}(\Theta \circ \nu)) \cup (C_2(\Theta \circ \nu) - \{L_2^1, \ldots, L_2^{r_2}\}(\Theta \circ \nu)) \end{aligned}$$

Lenže vieme, že $\lambda \circ \sigma$ je všeobecnejšie ako $\theta \circ \nu$, pretože λ je všeobecnejší unifikátor ako Θ a σ je všebecnejší unifikátor ako ν. Tým pádom C' je naozaj inštancia C.[16]
■

Veta 3.9.1 (Úplnosť metódy rezolvent) *Množina klauzúl S nie je splniteľná $\iff$ existuje odvodenie prázdnej klauzuly ε z S.*

Dôkaz:

C taká, že pre ľubovoľné inštancie C_1', C_2' je C' inštancia C". Inak povedané, C bude najvšeobecnejšia rezolventa a bude nezávislá od voľby základných inštancií C_1', C_2'.

[14] Poznamenávame, že C_1 a C_2 majú rôzne premenné a teda túto substitúciu získame ako zloženie individuálnych substitúcii pre jednotlivé klauzuly

[15] Pozor, zmizla nám čiarka z L_i oproti predchádzajúcej rovnici

[16] Ešte by sme mohli mať zlé svedomie z toho, čo na to povie množinové mínus, na ktoré sme v minulosti upozorňovali. Čitateľ sa môže sám presvedčiť, že v tomto prípade je to naozaj v poriadku

$\Leftarrow$: Budeme ukazovať sporom. Predpokladajme, že v S existuje odvodenie prázdnej klauzuly ε. Teda existuje postupnosť rezolvent $R_1, R_2, \ldots, R_n$ (medzi nimi niekde bude aj ε, zrejme môžeme predpokladať $R_n = \varepsilon$).

Kvôli sporu predpokladáme, že S je splniteľná, teda existuje jej model $\mathcal{M}$, ktorý vyhovuje všetkým klauzuliam z S. Ako sme predtým dokázali, pravidlo rezolventy je korektné pravidlo a teda, ak sú C_1, C_2 ľubovoľné klauzuly z S a C je ich rezolventa, zo splniteľnosti C_1, C_2 vyplýva aj splniteľnosť C. Ak teda prejdeme celé rezolvenčné odvodenie $R_1, R_2, \ldots, R_n$, postupne ukážeme, že $R_n = \varepsilon$ je splniteľná klauzula. Spor.

$\Rightarrow$: Ak predpokladáme, že S nie je splniteľná, potom podľa Herbrandovej vety (1. variant), nie je splniteľná práve vtedy, keď je možné jej priradiť konečný uzavretý sémantický strom T. Bez ujmy na všeobecnosti budeme ďalej predpokladať, že tento strom je binárny, teda každý vrchol má najviac dvoch synov.

Môže as stať, že strom T pozostáva jedine z koreňa – odmieta prázdnu klauzulu a v tomto prípade veta platí. Teraz predpokladajme, že strom T je konečný a má viac ako 1 vrchol. V tomto prípade má aspoň jeden akceptujúci vrchol.

Predpokladajme, že by tento strom nemal akceptujúci vrchol. Potom každý vrchol obsahuje nasledovníka, ktorý nie je odmietajúci. Tým pádom ale môžeme vytvoriť nekonečne dlhú vetvu, čo je spor s konečnosťou stromu T.

Množine $I(v)$ pre akceptujúci vrchol v zodpovedá čiastočná interpretácia končiaca v tom vrchole. Nech v_1, v_2 sú odmietajúci nasledovníci vrcholu v (spomeňme si na predpoklad, že strom je binárny). Čiastočné interpretácie $I(v)$, $I(v_1)$, $I(v_2)$ vyzerajú nasledovne:

$$\begin{aligned} I(v) &= \{m_1, m_2, \ldots, m_n\} \\ I(v_1) &= \{m_1, m_2, \ldots, m_n, m_{n+1}\} \\ I(v_2) &= \{m_1, m_2, \ldots, m_n, \neg m_{n+1}\} \end{aligned}$$

Zoberme teraz C_1' a C_2' (základné inštancie klauzúl C_1 a C_2), ktoré nie sú odmietnuté v $I(v)$ ale sú odmietnuté v $I(v_1)$ resp. $I(v_2)$. Potom C_1' musí obsahovať $\neg m_{n+1}$ a C_2' musí obsahovať m_{n+1}. Položíme $L_1' = \neg m_{n+1}$ a $L_2' = m_{n+1}$. Dostávame tak rezolventu

$$C' = (C_1' - L_1') \cup (C_2' = L_2')$$

o ktorej vieme, že musí byť nepravdivá v $I(v)$. Podľa predchádzajúcej lemy musí existovať rezolventa C taká, že C' je základná inštancia C.

Zoberme teraz nový sémantický strom T', ktorý dostaneme pre množinu $S \cup \{C\}$ tak, že odstrihneme strom T vo vrchole zodpovedajúcemu rezolvente C. Tento strom bude menší a teda opakovaním postupu sa nakoniec dostaneme až k stromu s jedným vrcholom. A o tom sme už prehlásili, že vtedy veta platí.

■

Príklad 3.9.6 Majme nasledujúce formuly:

$$\begin{aligned} F_1 &: (\forall x)(C(x) \to (W(x) \wedge R(x)) \\ F_2 &: (\exists x)(C(x) \wedge Q(x)) \\ G &: (\exists x)(Q(x) \wedge R(x)) \end{aligned}$$

Ukážte, že G je logickým dôsledkom F_1 a F_2.

Riešenie: Budeme ukazovať nesplniteľnosť $F_1 \wedge F_2 \wedge \neg G$. Pre F_1, F_2 a $\neg G$ vytvoríme štandardné formy. F_1 si upravíme takto:

$$\begin{aligned} (\forall x)(C(x) \to (W(x) \wedge R(x)) &\iff (\forall x)(\neg C(x) \vee (W(x) \wedge R(x)) \\ &\iff (\forall x)((\neg C(x) \vee W(x)) \wedge (\neg C(x) \vee R(x))) \end{aligned}$$

Štandardná forma je teda $\{\neg C(x) \vee W(x),\ \neg C(x) \vee R(x)\}$. Štandardná forma F_2 je $\{C(a),\ Q(a)\}$. Pre $\neg G$ dostávame

$$\neg G \iff \neg(\exists x)(Q(x) \wedge R(x)) \iff (\forall x)(\neg Q(x) \vee \neg R(x))$$

Štandardná formula pre túto formulu je $\neg Q(x) \vee \neg R(x)$

Dostávame nasledujúcich 5 klauzúl:

1 $\neg C(x) \vee W(x)$ – F_1

2 $\neg C(x) \vee R(x)$ – F_1

3 $C(a)$ – F_2

4 $Q(a)$ – F_2

5 $\neg Q(x) \vee \neg R(x)$ – G

Teraz budeme postupne robiť rezolventy:

6 $R(a)$ – rezolventa 2, 3

7 $\neg R(a)$ – rezolventa 4, 5

8 ε – rezolventa 6, 7

Záver: G je logickýkm dôsledkom F_1 a F_2.

3.10 Stratégia vymazávania

Na základe vety o úplnosti vieme, že ak máme nejakú množinu klauzúl S, tak viem z nej postupne vytvárať rezolventy a ak nie je splniteľná, po konečnom počte krokov dostávam prázdnu klauzulu ε. Za účelom dôkazu teda musíme zaradom prehľadávať všetky rezolventy, ktoré môže vzniknúť zo všetkých možných dvojíc klauzúl.

Príklad 3.10.1 Majme množinu klauzúl $S = \{P \vee Q,\ \neg P \vee Q,\ P \vee \neg Q,\ \neg P \vee \neg Q\}$. Metódou rezolvent ukážte, že S nie je splniteľná.

Riešenie: Použijeme takzvanú metódu nasýtenia – budeme postupne v každom kroku generovať najväčšiu možnú množinu rezolvent. Definujme si postupnosť $\{S^i\}_{i=0}^{\infty}$ množín klauzúl nasledovne: $S^0 = S$ a

$$S^{n+1} = \{\text{rezolventa klauzúl } C_1, C_2 \mid C_1 \in S^0 \cup S^1 \cup \cdots \cup S^n \wedge C_2 \in S^n\}, \quad n = 1, 2, \ldots$$

Takýmto spôsobom by sme po 39 krokoch dostali prázdnu klauzulu. Problém tejto metódy je, že niektoré klauzuly sa vyskytnú v popísanom prístupe viackrát. Prípadne sa tam môžu vyskytnúť tautológie.

Videli sme, že predchádzajúca metóda nie je úplne optimálna. Preto za účelom rýchlejšieho prehľadávania budeme niektoré evidentne nadbytočné rezolventy zahadzovať (a algoritmus nazveme stratégiou vymazávania). Najskôr si zadefinujeme, ako si budeme predstavovať nadbytočné rezolventy.

Definícia 3.10.1 (podklauzula) *Klauzula C je podklauzulou klauzuly D (alebo tiež C pohlcuje D) práve vtedy, keď existuje substitúcia σ taká, že platí $C\sigma \subseteq D$. Klauzulu D vtedy tiež nazývame nadklauzulou klauzuly C.*

Príklad 3.10.2 Majme klauzuly $C = P(x)$ a $D = P(a) \vee Q(a)$. Ak budeme uvažovať substitúciu $\sigma = \{a/x\}$, dostaneme $C\sigma = P(a)$ a teda $C\sigma \subseteq D$. Čiže C je podklauzula D.

Poznámka 3.10.1 *(:* Ak D je identicky rovná C alebo ak klauzula D je inštancia C, potom D je nadklauzula C. *:)*

Ako sme už teda povedali, stratégia vymazávania spočíva vo vylepšení metódy nasýtenia o zahadzovanie zbytočných výsledkov. Čiže opäť konštruujeme postupnosť $\{S^i\}_{i=0}$. Do S^{n+1} ale teraz vyberieme iba tie rezolventy C_1, C_2 (opäť $C_1 \in (S^0 \cup S^1 \cup \ldots \cup S^n)$ a $C_2 \in S^n$), ktoré nie sú tautológie a ani nadklauzuly niektorej z klauzúl dosiahnutej doteraz.

Príklad 3.10.3 (Revízia 3.10.1) Opäť máme množinu klauzúl $S = \{P \vee Q,\ \neg P \vee Q,\ P \vee \neg Q,\ \neg P \vee \neg Q\}$.

S^0 :
1 $P \vee Q$
2 $\neg P \vee Q$
3 $P \vee \neg Q$
4 $\neg P \vee \neg Q$

S^1 :
5 Q – rezolventa 1, 2
6 P – rezolventa 1, 3
7 $\neg P$ – rezolventa 2, 4
8 $\neg Q$ – rezolventa 3, 4

S^2 :
$\vdots$ – zahodíme veľa rezolvent, napr. rezolventa 1,8 je $P \vee \varepsilon \equiv P$ a tú už máme.
9 ε – rezolventa 5,8

3.10.1 Algoritmus pohltenia

Jediný problém, ktorý nám ostáva vyriešiť je detekcia či je nejaká klauzula tautológia alebo či je podformulou inej klauzuly. Prvý prípad sa rieši jednoducho – tautológiu máme práve vtedy, ak sa vo formule vyskytuje kontrárna dvojica. S podformulou to bude horšie. Skúsme sa na to pozrieť takto:

Nech C, D sú klauzuly. Označme si substitúciu premenných v D za nové konštanty (nevyskytujúce sa v C, D) ako

$$\Theta = \{a_1/x_1,\ a_2/x_2,\ \ldots,\ a_n/x_n\}$$

Ak je klauzula D tvaru

$$D = L_1 \vee L_2 \vee \ldots \vee L_m$$

dostávame, že $D\Theta$ je základná klauzula (neobsahujúca premenné).

$$D\Theta = L_1\Theta \vee L_2\Theta \vee \ldots \vee L_m\Theta$$

Nás bude zaujímať jej negácia

$$\neg D\Theta = \neg L_1\Theta \wedge \neg L_2\Theta \wedge \ldots \wedge \neg L_m\Theta$$

Algoritums, ktorý preveruje, či klauzula C je podklauzulou D bude vyzerať nasledovne:

1. Nech $W = \{\neg L_1\Theta, \neg L_2\Theta, \ldots, \neg L_m\Theta\}$ a nech $k = 0$ a $U^0 = \{C\}$
2. Ak U^k obsahuje ε, tak algoritmus skončí s výsledkom, že C je pod D.
3. V opačnom prípade kladieme
$$U^{k+1} = \{\text{rezolventa } C_1 \text{ a } C_2 | C_1 \in U^k \wedge C_2 \in W\}$$
4. Ak U^{k+1} je $\emptyset$, tak algoritmus skončí s výsledkom, že C nie je podklauzula D.

5. V opačnom prípade kladieme $k = k + 1$ a opakujeme krok 2

[FIXME: **Nasledujúca časť potrebuje skontrolovať a upraviť**]

Poznámka 3.10.2 *(: $\mathcal{U}^k$,$\mathcal{U}^{k+1}$, klauzuly z $\mathcal{U}^k$ sú konečné. $\mathcal{U}^0$,$\mathcal{U}^1$,... $\square$. :)*

Dôkaz: Predpokladajme, že C je podklauzula D. Na základe našej definície existuje substitúcia σ, že $C\sigma \subseteq D$. Teda $C(\sigma \circ \Theta) \subseteq D\Theta$. Literály z $C\sigma \circ \Theta$ môžeme vynechať pomocou jednotkových klauzúl z W. ... Algoritmus skončí svoju činnosť.

Obrátené tvrdenie: predpokladajme, že algoritmus zakončuje prácu na treťom kroku. Odmietnutie môžeme znázorniť nasledujúcim obrázkom:

[TODO: **obrazok**]

$$C_0, N_1, \ldots B_r \in W$$
$$C(\sigma_0 \circ \sigma_1 \circ \sigma \circ \sigma_r) = \{\neg B_0, \neg B_1, \ldots \neg B_r\} \subseteq D\Theta$$
$$\lambda = \sigma_0 \circ \sigma_1 \circ \sigma_2 \ldots \circ \sigma_r \rightarrow C\lambda \subseteq D\Theta$$

σ, ktorá dostaneme z λ tak, že v každom komponente λ nahradíme konštantu a_i premennou x_i, $i = 1, 2, 3, \ldots$. $C\sigma \subseteq D$. C je pod D. ■

Príklad 3.10.4 Majme

$$C = \neg P(x) \vee Q(f(x), a)$$
$$D = \neg P(h(y)) \vee Q(f(h(y)), a) \vee P(z)$$

Zistite, či klauzula C je podklauzulou D.

Začneme tým, že y a z sú premenné v D. Spravíme preto substitúciu $\Theta = \{b/y, c/z\}$ kde konštanty b, c nevystupujú v C ani D. Najprv vypočítame $D\Theta = \neg P(h(b)) \vee Q(f(h(b)), a) \vee \neg P(c)$ Čiže

$$\neg D\Theta = P(h(b)) \wedge \neg Q(f(h(b)), a) \wedge P(c)$$

A teda máme množiny

$$W = \{P(h(b)), \neg Q(f(h(b)), a), P(c)\}$$
$$U^0 = \{C\} = \{\neg P(x) \vee Q(f(x), a)\}$$

U^0 neobsahuje ε a teda musíme vytvoriť $\mathcal{U}^1$. Urobíme príslušnú substitúciu v množine $\mathcal{U}^0$. Dostávame nasledovné rezolventy:

$$U^1 = \{Q(f(h(b)), a), \neg P(h(b)), Q(f(c), a)\}$$

.

U^1 nie je prázdna a neobsahuje prázdnu klauzulu – musíme vytvoriť U^2. V tomto sa už vyskytne prázdna klauzula, čo znamená, že C pohlcuje klauzulu D.

Príklad 3.10.5 $C = P(x, x)$ a $D = P(f(x), y) \vee P(y, f(x))$. Zistite, či C je podklauzula D.

Riešenie (1) x, y sú premenné v D. a a b sú konštanty, ktoré sa nevyskytujú C, D. $\Theta = \{a/x, b/y\}$. $D\Theta = P(f(a), b), \vee P(b, f(a))$.

$$\neg D\Theta = \neg P(f(a), b) \vee \neg O(b, f(a))$$
$$W = \{\neg P(f(a), b), \neg P(b, f(a))\}$$
$$\mathcal{U}^0 = P(x, x)$$

(2) $\mathcal{U}^0$ neobsahuje $\square$, tak sa môže zistiť $\mathcal{U}^1$
(3) $\mathcal{U}^1 = \emptyset$. Záver: C nie je podklauzula D.

Príklad 3.10.6 Majme formuly:

1. $P \to S$
2. $S \to U$
3. P
4. U

Dokážte, že formula 4 vyplýva z formúl 1, 2 a 3.

Riešenie Prepíšeme si formuly do správneho tvaru, aby sme mohli použiť pravidlo rezolventy:

1. $\neg P \vee S$
2. $\neg S \vee U$
3. P
4. U

Snažíme sa nájsť negáciu – chceme ukázať, že

1. $\neg P \vee S$
2. $\neg S \vee U$
3. P
4. $\neg U$

nie je splniteľná. Zoberiem si rezolventu 1 a 3, dostávam S (5). Keď zoberiem 2 a 4, dostávam $\neg S$ (6). Zoberiem 5 a 6, dostávam $\square$ (7).

Príklad 3.10.7 Predpoklad: Študenti sú občania. Záver: Hlasy študentov sú hlasy občanov.

Riešenie

- $S(x)$ označuje „x je študent“.
- $C(x)$ označuje „x je občan“.
- $V(x, y)$ označuje „x je hlas y“.

Predpoklad: $(\forall y)(S(y) \to C(y))$. Študenti sú občania. Záver: $(\forall x)((\exists y)(S(y) \wedge V(x, y)) \to (\exists z)(C(z) \to V(x, z)))$. Hlasy študentov sú hlasy občanov.

Aká bude štandardná forma pre vyjadrenie predpokladu?

1. $\neg S(y) \vee C(y)$

   $\neg((\forall x)((\exists y)(S(y) \wedge V(x,y)) \rightarrow (\exists x)(C(z) \wedge V(x,z)))) \iff \neg((\forall x)(\forall y)(\neg S(y) \vee \neg V(x,y)) \vee (\exists z)(C(z) \wedge V(x,z))) \iff \neg((\forall x)(\forall y)(\exists x)(\neg S(y) \vee \neg U(x,y) \vee (C(z) \wedge V(x,z)))) \iff (\exists x)(\exists y)(\forall z)(S(y) \wedge V(x,y)) \wedge (\neg C(z) \vee \neg V(x,z))$ Teraz potrebujeme Skolemov normálny tvar: $(\forall z)(S(b) \wedge U(a,b)) \wedge (\neg C(z) \vee \neg V(a,z)))$

   Pre negáciu záver dostávane nasledujúce klauzuly:

2. $S(b)$
3. $V(a,b)$
4. $\neg C(z) \vee \neg V(a,z)$.
5. $C(b)$ z (1) a (2) (miesto y dosadíme b)
6. $\neg V(a,b)$ zo (4) a (5)
7. $\square$ z (3) a (6)

Predpokladajme, že b je študent, a je hlas študenta b a nie je hlas žiadneho občana. Pretože b je študent, b je občan. Okrem toho a nemôže byž hlas b, pretože b je občan a to nie je možné.

Kapitola 4

Neodprednášané v šk. roku 09/10

Nasledujúca kapitola obsahuje veci, ktoré neboli odprednášané doc. Tomanom v roku, keď som dôkladne prerábal tieto poznámky. Evidentne ale dané veci boli odprednášané rok predtým, odkiaľ sú aj nasledujúce poznámky. Na začiatku by to chcelo snáď upozornenie, že dané poznámky sú neoverené a z predchádzajúcich skúseností môžu byť chaotické a neúplné (i keď základný obsah majú zachytený dobre).

Poprosil by som preto, ak máš poznámky k tejto časti, bolo by najideálnejšie, ak by si vygeneroval/-a pripomienky k skriptám a buď doručil/-a mne osobne alebo rovno prepísal/-a zdrojové kódy skript. Myslím, že Ti za to budú vďačné budúce generácie.

PPershing

[FIXME: **Nasledujúca časť potrebuje skontrolovať a upraviť**]

4.1 Rozširovanie teórie

Veta Nech A je formula teórie T s jazykom L, nech všetky voľné premenné formuly A sú $x_1, x_2, \dots x_n$, ďalej nech L' je rozšírenie L pridaním nového predikátového symbolu P a nech T' vznikne z T pridaním axiomy $P(x_1, \dots x_n) \iff A$ (označme ju *).

Potom teória T' s jazykom L' je konzervatívne rozšírenie teórie T s jazykom L. Ďalej, pre každú formulu B jazyka L' existuje formula B^* z jazyka L, že platí $T \models B \iff B^*$.

Najprv budeme konštruovať B^*. Dôkaz: Nech B je formula na jazyku L', nech A' je variant formuly A (definujúcej predikát P), že žiadna premennáz formuly B nie je viazaná vo formule A'.

Nech B^* vznikne z B tak, že každú podformulu $P(a_1, \dots a_n)$ nahradíme podformulou $A'(a_1, \dots a_n)$ a podľa vety o variantoch nám platí, že:

$$T' \models P(a_1, \dots, a_n) \iff A'(a_1, \dots a_n)$$

$$T' \models B \iff B^*$$

.

Ukážeme, že T' v jazyku L' je konzervatívne rozšírenie teórie T v L (teda pre ľubovoľnú formulu na pôvodnom jazyku, ktorá je dokázateľná v teórii L', je dokázateľná aj v pôvodnej teórii – nevzniknú žiadne nové teorémy). Nech C je ľubovoľné formula na jazyku L', ďalej nech platí $T' \models C$. Nám stačí dokázať, že $T \models C^*$. Ak je potom formula C na jazyku L, potom C^* je C.

Uvažujme $C_1, C_2, \dots C_n$ je odvodenie formuly C v teórii T'. Nám stačí ukázať, že C_i^* sú dokázateľné (odvoditeľné) v T.

Pri odvodení C sa môže stať nasledovné:

1. C_i je axioma predikátovej logiky L, potom C_i^* je axioma rovnakého druhu

2. C_i je axioma z T, potom C_i^* je C_i a teda je dokázateľná z T.

3. Môže sa stať, že C_i je axioma (x) $P(x_1, \ldots, x_n) \iff A(x_1, \ldots, x_n)$.
   $C_i^* : A_i \iff A_i$, je dokázateľná pomocou vety o variantoch.

4. Ak C_i je odvodená z C_j a C_k, použijeme pravidlo modus ponens. C_i^* je odvodené z C_j^* a C_k^* tým istým pravidlom.

5. C_i je odvodené z C_k pravidlom zovšeobecnenia ($k < i$). Potom C_i^* je odvodené z C_k^* pomocou toho istého pravidla.

Ak máme teóriu T a každá jej $A \in T$ je otvorená (každá premenná je voľná), hovoríme o otvorenej teórii.

Majme danú teóriu T s jazykom L. Máme k nej zostrojiť teóriu T_H (henkinova teória) s jazykom $L(C)$, kde C je zjednotenie konštánt všetkých rádov. Dôležité pre nás budú konštanty $c_A, c_{\neg A}$.

- $A_{c_{\neg A}} \to (\forall x)A$ (*)
- $(\exists)A \to A(c_A)$ (**)

$$A \iff \neg\neg A$$
$$c_{\neg A} \iff \neg A(x)$$
$$\neg A(c_{\neg\neg A}) \to (\forall x)\neg A$$
$$(\exists x)A \to A(c_{\neg\neg A})$$

(Použili sme prenexnú operáciu).

Ak $c_{\neg A}$ je konštanta z axiomy s (*), tak hovoríme, že prislúcha (patrí) formule A. Keď zoberieme formulu A.

$$(\forall x)A \to A(t)$$

– t je term bez premenných v $L(C)$

$$A_{[c_{\neg A}]} \to (\forall x)A.\ldots\ldots c_{\neg A}$$

$\delta(T)$ množina na jazyku $L(C)$ prislchajúu konštante C má ... axiomy identity a ... a formúl z T.

Lema 1 Nech A je formula na jazyku L a ďalej, nech A' je uzavretá inštancia formuly A na jazyku $L(C)$. Ak platí, že formula A je dokázateľná v pôvodnej teórii, potom A' je tautologickým dôsledkom konečne mnoho formúl z $\delta(T)$

Dôkaz Nech $A_1, A_2, \ldots, A_n$ je dôkaz formuly A v teórii T. Indukciou podľa dĺžky dôkazu ukážeme, že ľubovoľná uzavretá formula v jazyku $L(C)$ inštancia A'_j formuly A_j je tautologickým dôsledkom konečne veľa formúl z $\delta(T)$.

Môžu nastať tieto prípady:

- A_j je axioma výrokovej logiky. Potom A'_j je opäť tautológia. A je tautologickým dôsledkom prázdnej množiny predpokladov.
- A_j je axioma tvaru $(\forall x)B \to B_x[t]$. Axioma špecifikácie. $A_j : (\forall x)B' \to B'_x[t]]$ – leží v δT. t' je term bez premenných a je v $L(C)$.

- A_j je axioma $(\forall x)(C \to D) \to (C \to (\forall x)D)$, x nie je voľná v C.

  Uvažujme formulu $(\forall x)(C \to D) \to (C \to (\forall x)D_x[c_{\neg D}])$. Táto formula patrí to $\delta(T)$, lebo je to inštancia axiomy špecifikácie.

  $D_x[c_{\neg D}] \to (\forall x)D$ – opäť patrí do $\delta(T)$ (opäť (*))

  Tvrdíme, že formula A_j je tautologický dôsledok horeuvedených formúl. Budeme uvažovať takúto formulu: t – $(A_1 \to (B_1 \to D_1)) \to ((D_1 \to C_1) \to (A_1 \to (B_1 \to C_1)))$ Tvrdíme, že táto formula je teoréma.

  Dôkaz formuly: Za predpoklady si zoberiem formuly $A_1, (A_1 \to (B_1 \to D_1)), B_1, (D_1 \to C_1)$. Z týchto predpokladov dokážem odvodiť C_1.

  A_1 bude formula $(\forall x)(C \to D)$, $B_1 : C$, $C_1 : (\forall x)D$, $D_1 : D_x[c_{\neg D}]$

- A_j je axioma z T, potom $A'_j \in \delta(T)$.

- A_j je axioma identity alebo axioma rovnosti, potom A'_j patrí do $\delta(T)$.

- A_j dostaneme aplikáciou pravidla modu ponens z formúl A_k a A_l, pričom $k, l < i$. A'_j dostávame z A'_k a A'_l pomocou pravidla modus ponens.

- A_j je odvodená z A_k pravidlom zovšeobecnenia, pričom predpoklad je $k < j$. Teda $A_j : (\forall x)C$, teda $A_k : C$, x – premenná. Inštancia $A'_j : (\forall x)C'$. Uvažujme inštanciu A'_k formuly A_k v takomto tvare: $A_k : C'_k[c_{\neg C'}]$. Podľa indukčného predpokladu je táto formula tautologickým dôsledkom konečne veľa formúl z $\delta(T)$. Uvažujme formulu

  $$C'_x[c_{\neg C'}] \to (\forall x)C' \qquad (***)$$

  A'_j je tautologickým dôsledkom formuly z $\delta(T)$. Dokázali sme formulu A' tak, že sme nepoužili pravidlo zovšeobecnenia.

Definícia Hovoríme, že formula A je kvázitautológia, ak je tautologickým dôsledkom inštancií axiom identity a rovnosti.

Veta (Hilbert-Ackermann) Otvorená teória T v jazyku L (s rovnosťou) je sporná práve vtedy, keď existuje (kvázi-)tautológia, ktorá je disjunkciou negácií inštancií axiom z T.

Dôkaz Najprv ľahšia implikácia: Predpokladajme, že sú splnené podmienky vety, tak potom T je sporná. Zoberme si nejakú formulu A. Berieme $\neg A_1 \vee \neg A_2 \vee \ldots \vee \neg A_n$, kde A_i sú inštancie axiom z T. Pomocou de Morganovho zákona dostaneme $A_1 \wedge A_2 \wedge \ldots \wedge A_n$. Ak platí $T \models A_i$, potom $T \models A_1 \wedge \ldots \wedge A_m$, a teda T je sporná, lebo je z nej dokázateľná ľubovoľná formula B, pretože $\models A \to (\neg A \to B)$ a $T \models B$.

Naopak: Predpokladajme, že otvorená teória T je sporná. $x \neq x$, $T \models x \neq x$. Z toho vyplýva, že ak si zoberieme ľubovoľnú konštantu $r \in C$, tak potom dostávame inštanciu formuly: $r \neq r$. To je uzavretá inštancia teorémy vety z T, čiže podľa Lemy 1 eistuje $A_1, A_2, \ldots A_k$ z $\delta(T)$ také, že $r \neq r$ je tautologickým dôsledkom A_1 až A_k, teda z predpokladov inštancií je dokázateľné $A_1, A_2, \ldots, A_k \models r \neq r$. Platí $A_1 \to A_2 \to \ldots \to A_k \to r \neq r$ – tautológia. $p \to q \iff \neg p \vee q$. $\neg A_1 \vee \neg A_2 \vee \ldots .. \vee \neg A_k \vee \neg(r = r)$ je tautológia. A_i sú inštancie z $\delta(T)$. Posledná formula je tautológia, ktorá je disjunkciou negácií inštancií z $\delta(T)$.

Definícia Postupnosť formúl $A_1, A_2, \ldots A_n$ nazveme špeciálnou, ak $\neg A_1 \vee \neg A_2 \vee \ldots \vee \neg A_n$ je tautológia. (Vieme) Ak T je sporná teória, potom existuje špeciálna postupnosť z $\delta(T)$

(pokračovanie)

Definícia Stupeň konštanty $c_{\neg A}$. $(\forall x)A$ uzavretá formula na jazyku $L(C)$. Hovoríme, že konštanta $c_{\neg A}$ spojená axiomou

$$A_{c_{\neg A}} \to (\forall x)A$$

s formulou $(\forall x)A$ je stupňa n, ak formula $(\forall x)A$ obsahuje n výskytov kvantifikátorov $\forall$ alebo $\exists$.

Množina formúl $\delta_n(T)$ vznikne z $\delta(T)$ vynechaním všetkých formúl stupňa $> n$ pre konštantu $c_{\neg A} \in C$. Treba si uvedomiť, že stupeň konštanty $c_{\neg A}$ je vždy aspoň 1. $\delta_0(T)$ – uzavreté inštancie, axiomy z množiny T a axiom identity a rovnosti.

(Dokázali sme) Ak teória T je sporná, existuje špeciálna postupnosť, ktorá patrí do $\delta(T)$. Nech n je najmenšie také n, že špeciálna postupnosť z $\delta(T)$ je obsiahnutá v $\delta_n(T)$:

$n = 0$. Musíme nájsť špeciálnu postupnosť prislúchajúcu do T. Predpokladáme, že pre $n = 0$ máme postupnosť $A_1, A_2, \dots A_k$ – špeciálna a patrí do $\delta_O(T)$. $c_A, c_{\neg A}$ nahradíme pomocou premenných $A'_1, A'_2, \dots A'_k$ (opäť špeciálna postupnosť). $A'_1, A'_2, \dots, A'_n$ sú všetky formuly, ktoré patria do T. $A'_1, A'_2, \dots A'_k$ budú inštancie axiom identity a rovnosti. $\neg A'_1 \vee \neg A'_2 \vee \dots \vee \neg A'_n \leftarrow A_{n+1} \leftarrow \dots \leftarrow A'_k$ – kvázitautológia (vyplýva z toho, že táto postupnosť je špeciálna). $A'_1, A'_2, \dots A'_n \in T$.

Lema Ak $n > 0$ a existuje špeciálna postupnosť z $\delta_n(T)$, tak potom existuje špeciálna postupnosť aj z $\delta_{n-1}(T)$.

Dôkaz (pokračovanie dôkazu) Hilbert-Ackermanovej vety. $\delta_0(T)$. Vieme vytvoriť postupnosť $B_1, B_2, \dots, B_q \in T$.

Poznámka Elementárna aritmetika je otvorená teória s konečným počtom axiom. Hilbertova arigmetika, Presburgerova (??) aritmetika (aritmetika so symbolmi $0, S, +$. Peanova aritmetika (1931).

Definícia

1. Hovoríme, že formula A je existenčná, ak A je v prenexnom tvare a všetky kvantifikátory v prefixe sú existenčné .
2. Hovoríme, že formula A je univerzálna, ak A je v prenexnom tvare a všetky kvantifikátory sú univerzálne.

Lema 3 Uzavretá existenčná formula A je dokázateľná v predikátovej logike (s rovnosťou) práve vtedy, keď istá disjunkcia otvoreného jadra formuly A je kvázitautológia.

Dôkaz $A : (\exists x_1)(\exists x_2) \dots (\exists x_n)B$ –formula v prenexnom tvare, B je otvorené jadro.

1. Formulá A je dokázateľná $\iff$ teória s jedinou špeciálnou axiomou $\neg A$ je sporná.
2. Ak použijeme prenexné operácie, dostávame $\models \neg A \iff (\forall x_1) \dots (\forall x_n)\neg B$. $\neg A \iff (\forall x_1) \dots ({}_n)\neg B$.
3. Formula A je dokázateľná $\iff$ keď teória T s jedinou špeciálnou axiomou $\neg B$ je sporná. $\neg B$ je otvorená. Keď použijeme Hilbert-Ackermannovu vetu, dostávame $\neg B_1, \neg B_2 \dots, \neg B_m$ – nad $\neg B$. Platí $\neg\neg B_1 \vee \neg\neg B_2 \vee \dots \vee \neg\neg B_m$, čo je to isté ako $B_1 \vee B_2 \vee \dots \vee B_m$, čo je to isté, ako Hilbert-Ackermannova veta.

Teóriu T rozširujeme do T_H s jazykom $L(C)$ a tú zase do T_R s $L(C)$. $A_x[C_{\neg A}] \to (\forall x)A$ – toto môžeme aj obrátiť:

$$(\forall x)A \to A_x[c_{\neg A}]$$

– vďaka axiome špecifikácie.

Ak teraz vezmeme formulu B takú, že $A \iff B$, potom platí $B_x[c_{\neg B}] \to (\forall x)B$.

$$\begin{array}{lll} T_H & \models & A_x[c_{\neg A}] \iff B_x[c_{\neg B}] \\ T_H & \models & A_x[c_{\neg A}] \iff (\forall x)A \\ T_H & \models & A \iff B \\ T_H & \models & (\forall x)A \iff (\forall x)B \\ T_H & \models & B_x[c_{\neg B}] \iff (\forall x)B \end{array}$$

$$(\forall x)(A \iff B) \to c_{\neg A} = c_{\neg B}$$

Lema 4 Pre ľubovoľnú teóriu T je T_R konzervatívne rozšírenie.

Majme formulu A, ktorá je uzavretá a napísaná v prenexnom tvare. Indukciou podľa počtu všeobecných kvantifikátorov budeme formulu transformovať do tzv. Herbrandovho variantu. Ak formula A má tvar:

$$A : (\exists x_1) \dots (\exists x_n)(\forall y)B, \qquad n \geq 0$$

$$A^* : (\exists x_1) \dots (\exists x_n)B_y[f(x \dots x_n)]$$

, A^* je A_H

$A^{**}, L \cup \{f, g, h, \dots\}$.

Veta (Herbrandova) Uzavretá formula v prenenom tvare je dokázateľnáv predikátovej logike (s rovnosťou) práve vtedy, keď istá disjunkcia inštancií otvoreného jadra je kvázitautológia.

Dôkaz A_H – je existenčná formula. Je dokázateľná práve vtedy, keď vezmeme do úvahy lemu 3 a platí formulácia našej vety. L' .... ??? . Stačí ukázať, že:

$$\models_L A \iff \models_{L'} A_H$$

. Implikácia zľava doprava je ľahšia – vieme ukázať, že $\models_{L'} A \to \models_{L'} A^*$. Premennú y sme nahradili funkciu n premenných. Všimnime si:

$$\models_{L'} (\forall y)B \to B_y[f(x_1 \dots x_n)]$$

; axioma špecifikácie. $(\exists x_1)(\exists x_2), \dots (\exists x_n)$. Potom platí aj $\models A \to B$, $\models (\exists x)A \to (\exists x)B$

Veta (o zavedení funkčného symbolu) Nech formula $(\exists y)A$ je dokázateľná v teórii T s jazykom L. Nech $x_1, x_2, \dots, x_n$ sú všetky voľné premenné, ktoré sa vyskytujú vo formuli $(\exists y)A$. Nech T' vznikne z T pridaním nového n-árneho funkčného symbolu f a pridaním axiomy $A_y[f(x_1, \dots, x_n)]$. Potom T' je konzervatívne rozšírenie teórie T.

Dôkaz Nech B je uzavretá formula teórie T (s jazykom L). Predpokladáme, že B je teorémou (vetou teórie) T'. $T' \models B$. Máme ukázať, že aj v $T \models B$. Predpokladajme, že formula B má dôkaz v T' a že v tom dôkaze vystupujú $a_1, a_2, \dots, a_n$ – špeciálne axiomy teórie T, prípadne axioma $(*)$. Na základe tohto predpokladu je v predikátovej logike dokázateľná nasledovnaá formula.

$$(1) \models (\forall x_1)(\forall x_2) \dots (\forall_n)a_y[f(x_1 \dots x_n)] \to B_1 \to B_2 \to \dots \to B_n \to B$$

$B_1, \dots, B_n$ sú ...ny funkcií $A_1, A_2, \dots, A_n$.

$$A_y[f(x_1, \dots x_n)], A_1, \dots, A_n \models B$$

Označme si C – prenexný tvar nasledovnej formuly:

$$A \to B_1 \to \dots \to B_n \to B$$

Potom:

$$(2)(\exists x_1)(\exists x_2)\dots(\exists x_n)C_y[f(x_1,\dots,_n)]$$

je prenexný tvar (1)

Uvažujme $D : (\exists x_1)\dots(\exists x_n)(\forall y)C$. Potom z tohto vyplýva D je formula jazyka L a neobsahuje novo zavedený symbol f. Ak konštruujeme herbrandovský variant tej podformuly (D_H) (meníme veľké kvantifikátory) a na prvom kroku dostávame $D^* : (\exists x_1)\dots(\exists x_n)C_y[f(x_1,\dots x_n)]$ – prenexný tvar (1). Z Herbrandovej vety dostávame, že D^* je dokázateľné, z tadiaľ $(D^*)_H$ je dokázateľné a z toho $(4)T \models D$

Prenexnými operáciami dostávame

$$(5)(\exists x_1)(\exists x_2)\dots(\exists x_n)(\forall y)(A \to B_1 \to \dots \to B_n \to B)$$

$$(6)T \models (\forall x_1)(\forall x_2)\dots(\forall x_n)(\exists y)A \to B_1 \to B_2 \to \dots \to B_n \to B$$

Každý z týchto predpokladov je dokázateľný v T, dostávame $T \models B$ a teda T' je konzervatívne rozšírenie B.

Mám formulu A, ktorá je uzavretá, idem priradiť skolemov tvar (skolemov variant).

1. Ak formula A je univerzálna, potom A_S je formula A
2. Ak A je tvaru $(\forall x_1)\dots(\forall x_n)(\exists y)B, n \geq 0$, f je funkčný symbol, kladieme $A_S : (\forall x_1)\dots(\forall x_n)B_y[f(x_1,\dots,x_n)]$, $(A')C$...

(1*) $A' \models A$ a ... $A_S \models A \models B_y[f(x_1,\dots,x_n)] \to (\exists y)B$ – duálny tvar axiomy špecifikácie. Teraz môžeme sformulovať Skolemovu vetu:

Veta (Skolemova) V ľubovoľnej teórii T môžeme zostrojiť otvorenú teóriu T', ktorá je konzervatívnym rozšírením teórie T.

Dôkaz Mám teóriu T s jazykom L. Zostrojím si teóriu T_1 s tým istým jazykom a tá teória T_1 sú uzávery prenexných tvarov axiom z T. Z vety o uzávere a vety o prenexnom tvare platí, že T_1 je konzervatívne rozšírenie T a naopak, T je konzervatívne rozšírenie T_1. $T \equiv T_1$.

Teória T_2 vznikne z teórie T_1 tak, že ľubovoľnej formuli $A \in T_1$ zostrojíme skolemov variant A_S. V T_2 je konzervatívne rozšírenie T_1 podľa vety o zavedení funkčného symbolu.

Ideme vytvárať teóriu T_3 – vznikne z T_2 vynechaním všetkých axiom z T_1. Podľa (1*) dostávame, že $T_2 \equiv T_3$.

Ďalej vytvárame teóriu T_4 – pozostáva z otvorených jadier T_3, teda $T_3 \equiv T_4$. Keď to zhrnieme, dostávame: $T \equiv T_1$, T_2 je konzervatívne rozšírenie T_1. $T_2 \equiv T_3 \equiv T_4$, a z toho T_4 je konzervatívne rozšírenie T.

Veta (o zavedení funkcie pomocou definície) Majme teóriu T s jazykom L a nech $x_1,\dots,x_n,y$ sú navzájom rôzne premenné, ktoré sa vyskytujú voľne vo formule D. Nech platí:

1. $T \models (\exists y)D$
2. $T \models D \to (D_y[y] \to y = t)$

Nech L' vznikne z L pridaním nového n-árneho funkčného symbolu f a T' z T pridaním axiomy

$$(3)y = f(x_1,\dots x_n) \iff D$$

(definícia axiomy). Potom T' je konzervatívne rozšírenie T a ku každej formule A na jazyku L' existuje formula A^* na jazyku L taká, že platí

$$(4)T' \models A \iff A^*$$

Dôkaz Najprv ukážeme, ako ku formuli A priradiť formulu A^*, a potom ukážeme, že T' je konzervatívne rozšírenie T.

Zostrojíme A^* z A tak, aby platilo (4). Formulu A máme na jazyku L', problematický je symbol f – vyskytuje sa v atomických podformuliach. Nech funkčný symbol f sa vyskytuje vo formuli A a nech je to ten najvnútornejší výskyt. Je to nejaký $f(t_1, \dots t_n)$, pričom $t_1, \dots, t_n$ už neobsahujú f.

$$A : B_z[f(t_1, \dots, t_b)]$$

, a naše z sa nevyskytuje vo formuli A, a ani v definujúcej formuli D. Položme A^* tvare:

$$(5)(\exists z)D'_{x_1,\dots,x_n,y}[t_1, \dots, t_n, z] \wedge B^*)$$

, pričom D' je variant D, v ktorej nie je viazaná žiadna premenná, ktorá sa vyskytuje vo formuli A. Z vety o variantoch a definujúcej axiomy (3) dostávame, že na jazyku L' je dokázané (6) $\models_{L'}$ $z = f(t_1, \dots, t_n) \iff D'[t_1, \dots t_n, z]$. Z vety o ekvivalencii dostávame, že platí

$$(7)T' \models (\exists z)z = f(t_1, \dots, t_n) \wedge B^*) \iff f^*$$

. Z indukčného predpokladu dostávame

$$(8)T' \models B \iff B'$$

$$(1)T' \models (\exists z)(z = f(t_1, \dots, t_n) \wedge B) \iff A^* \text{ z vedy o } \dots . (\models (\exists x)(x = t \wedge A) \iff A_x[t])$$

$$T' \models B_z[t_1, \dots, t_n] \iff A^*$$

, na ľavej strane je formula $A : B_z[t_1, \dots t_n]$.

Použijeme vetu o zavedení funkčného symbolu. Uvažujme S – teóriu z jazyka L', ktorá vznikne z T pridaním axiomy:

$$(10)D_y[f(x_1, \dots, x_n)]$$

.

Ukážeme, že T' a S sú ekvivalentné a platí $T' \equiv S$. Potrebujeme ukázať, že (10) je teorémou T' a $(3)y = f(x_1, \dots, x_n) \iff D$ je teorémou (vetou) S. V $T' \models f(x_1, \dots x_n) = f(x_1, \dots ,_n) \rightarrow D_y[f(x_1, \dots_n)]$, formula je inštancia axiomy (3). Ak použijeme inštanciu na axiomu identity (3) $T' \models D_y[f(_1, \dots, x_n)]$. Potrebujeme ukázať, že 3 je dokázateľná v S. Vyjdeme z tvaru (11) $\models_{L'}$ $y = f(x_1, \dots x_n) \rightarrow (D \iff D_y[f(x_1, \dots, x_n)])$.

$$(12) \models_{L'} D_y[f'(x_1, \dots, x_n)] \rightarrow (y = f(x_1, \dots_n \rightarrow D)$$

$$(13)S \models (y = f(x_1, \dots, x_n) \rightarrow D) \text{ z } (10)$$

$$(14) \models_{L'} D_y[f(x_1, \dots, x_n)] \rightarrow (D \rightarrow y = f(x_1, \dots x_n)][T \models D \rightarrow [D_y[t] \rightarrow y = t)(2)$$

$$S \models D \rightarrow y = f(x_1, \dots x_n)$$

Kapitola 5

Skúška

5.1 Písomná časť na konci semestra

Na konci semestra existuje k predmetu písomka. Táto písomka by sa mala skladať z 5 príkladov.

1. Preniesť formulu do prenexného tvaru. Ako podotázka môže byť dôkaz niektorej z prenexných operácii.
2. Napíšte axiómy nejakej teórie s rovnosťou, jej jazyk, špeciálne symboly a model (napríklad Teória telies alebo grúp)
3. Dokážte Lindenbaumovy/Henkinovu/inú z ľahších viet počas semestra. Prípadne niečo na štýl "definujte konzervatívne rozšírenie + príklad". Táto otázka je teoretická otázka.
4. Daná je množina S. Nájdite unifikátor, Skolemov tvar. Proste, nejaká úloha z automatického dokazovania.
5. Metódou rezolvent ukážte nesplniteľnosť zadanej množiny klauzúl S.

5.2 Samotná skúška

[FIXME: **Nasledujúca časť potrebuje skontrolovať a upraviť**]

- Dokázať 4 vety
- je daná formula, nájsť prenexný tvar, skolemov tvar, metódou rezolvent ukázať, či platí alebo neplatí, napíšte teóriu s rovnosťou
- 3 alebo 4 definície

Koniec neoverenej časti
